بسم الله الرحمن الرحيم

((مَنْ عَمِلَ صَالِحًا مِّن ذَكَرٍ أَوْ أُنثَى وَهُوَ مُؤْمِنٌ فَلَنُحْيِيَنَّهُ حَيَاةً طَيِّبَةً وَلَنَجْزِيَنَّهُمْ أَجْرَهُم بِأَحْسَنِ مَا كَانُواْ يَعْمَلُونَ)) (٩٧) سورة النحل.

كتاب بعنوان ::

احتراف أمن وحماية الأجهزة الشخصية

موجه للمستخدم العادي ذو الخبرة البسيطة

في استخدام الأجهزة الشخصية ..

إعداد :: محاضر دورة احتراف أمن وحماية الأجهزة الشخصية

حماد حجازي (أبو موسى)

جوال :: 00970599861963

البريد الإلكتروني :: z83@live.com

فلسطيـن – غزة

3/2011 - الطبعة الأولى

الفهرس

المحتويات

إهـــــداء

أهدي هذا الكتاب إلى :

الأمة الإسلامية وجميع الإنسانية

على أمل أن نرى في واقع هذا العالم دولة
فلسطينية مستقلة محررة، لا تهم
المساحة والحدود، ولا تهمنا أوضاع أهلها
الاقتصادية، ولكن ما يهمنا مثلما هم
والدنا ورمزنا وقائدنا رحمه الله وأسكنه
فسيح جناته : ياسر عرفات

أن تكون القدس عاصمتها،

وأن تلتحم طاقات جميع أحزابها وأفرادها
لبنائها والعمل على تحقيق الحلم الذي
استشهد من أجله الكثيـــر وما توفيقنا إلا
بالله العلي العظيم ..

المقدمــة

سأبدأ قائلاً أن عدد مستخدمي الانترنت قد بلغ في شهر فبراير عام ٢٠١١ تقريبا ٢ مليار مستخدم ، تستطيع الوصول لأي مستخدم منهم على أي شبكة في العالم وفي أي دولة في وقت لا يكاد يذكر ، هذه التكنولوجيا التي انتشرت سريعاً ومازالت تحقق أرقاما قياسية في الانتشار كان لا بد من توظيفها جيداً لتستثني المستخدمين الذين قد يضرون غيرهم بأهداف كثيرة .

لكن هذا لم يحدث فالمجرمين يتعقبون كل الوسائل التي تم إنتاجها أو سيتم بهدف تنفيذ هجماتهم التي قد تضر بفئة دون أخرى وقد تستهدف بشكل عشوائي ، وقد تكون موجهه لفرد واحد فقط .

ولما كان هذا ، كان لا بد للمستخدم الذي يواظب على استخدام الانترنت ويفيد ويستفيد أن يتعلم أساليب حماية نفسه في هذا العالم الضخم ، والذي قد يحوله من شخص باحث إلى شخص مبحوث عنه ..

بمعنى أن أغلب من يدخلون الانترنت يبحثون وتشير التقارير إلى أن مستخدمي الانترنت يجرون أكثر من مليار عملية بحث أسبوعيا في موقع البحث قوقل فقط ..

من يتم استهداف جهازه واختراقه ، فقد يتم إلحاق الضرر به بالأشكال التالية ::

١ – تحميل ونشر صور خاصة موجودة فعلياً على الجهاز ..

٢ – تسجيل ونشر فيديو أو صوت يتم التقاطه من الشخص المستهدف .

٣ – تسجيل ونشر كتابات قد يقوم بتنفيذها ولا يريد لأحد الإطلاع عليها.

٤ – سرقة حساباته على البريد الالكتروني أو المواقع الاجتماعية واستخدام البريد المسروق في جلب ضحايا آخرين مضافين لدى الشخص المستهدف .

٥- سرقة معلومات بنكية وبالتالي إلحاق الضرر مادياً بالشخص المستهدف .

٦ – تدمير المعلومات الخاصة والوثائق وزرع مختلف أنواع الفيروسات والديدان التي يتم ابتكارها يومياً لإلحاق أكبر الضرر في الأجهزة المستهدفة .

٧ - استخدام الجهاز المستهدف في عمليات التحايل والاختراق الإجرامي الذي قد يوجه إلى مواقع حكومية أو مؤسساتية .

كثيرة هي الأسباب التي تتطلب منا كـ عرب الوثوق بأمان جهازنا الشخصي والمحافظة على كافة تعاملاتنا على الإنترنت أو داخل الجهاز الشخصي بشكل يمثل قمة الخصوصية وذلك لعدة أسباب أهمها ديننا وتقاليدنا العربية ، فقد نرى أن كثير من الهاكرز العربي يستخدم الاختراق في استهداف أبناء عروبته حتى يتجسس على أفعالهم وينشر زلاتهم ، وحتى المستخدم العادي الذي قد يكون مخترقاً ويتم التسجيل عليه نجده يكتب في أغلب عمليات البحث التي تجري على الشبكة كلمة (فضيحة) ، وتشير بعض الإحصائيات إلى أنها من بين أكثر الكلمات التي يتم البحث عنها عربيـــاً !!!

وحينها وجب أن نستذكر ها هنا الحكمة القديمة ::

كَمَا تدِينُ تُدَانُ

لذا إن كنت تتعلم وتنطلق بين المنتديات لتتعلم هذا العلم لتتبع عورات إخوانك العرب فسارع للخروج من حلقة العلم هذه ، واحرص على ألا تعود لأني دعوت ورجوت الله عز وجل أن يعجل بعقاب من يستخدم هذا العلم في ما يضر أي إنسان وليس المسلمين فحسب ..

أرجوكم إخواني وأخواتي الكرام أن نحافظ على سنن من سبقنا وان نغير ما استطعنا في واقعنا العربي الحالي ، ولنبحث دائما عما يعيننا على قضاء أمورنا وحاجتنا ، ونبتكر أساليب لنشغل أوقاتنا بأي شيء من شأنه التقليل ومن ثم منع البحث عما يغضب الله ، واعلم أخي الكريم أن الكثيرين يحتاجونك فكما ستتعلم إن شاء الله حاول أن تعلم وان تثقف من حولك في هذا العلم حتى لا يقع أحداً بإذن الله بين فكي الشياطين الذين يتكاثرون يوماً بعد آخر وأصبحوا ينجسون صفحات الانترنت وخيراته ، فبعزة الله وجلاله قد يستخدم هؤلاء البرامج الإسلامية وقد يستخدم آخرين مواقع تعليم البرامج أو نشر الأفلام العادية والأغاني وغيرها الكثير فالحذر الحذر ..

تابعوا معنا وبإذن الله لن أبخل في أي شيء ،،

وسأحاول تبسيط المعلومة قدر ما أستطيع ، ومن يريد أي شرح إضافي فليراسلني وبإذن الله سأقف معه وسأوضح له ما يريد بالوسائل المتاحة وفي أي قسم من الأقسام إلا القسم الخاص بالحديث عن الهاكرز ، وذلك لأنه قسما أضفته حتى يتمكن الدارس من معرفة أساليب الهاكرز في استدراج ضحاياه ، ومعرفة البرامج المستخدمة وكيفية استخدامها حتى يطور نفسه ويتعلم أي أساليب جديدة أخرى في

حال تطور الهاكرز وانتهى زمن العمل ببعض أجزاء الكتاب فالبحث المستمر مطلوب ، وإن شاء الله سأستمر بتطوير الكتاب وتحديثه بشكل مستمر .

وأشكر كل من سينبهني إلى إضافة معينة يتمنى طرحها في الإصدار القادم ..

أو أسلوب آخر في تصميم وعرض وشرح بعض الأمور .

أو خطأ قد ارتكبه في بعض التطبيقات ، لاني لست بمعصوم .

وفقنا الله جميعـاً ،،

اللهم اغفر لي ولوالدي ولقارئي الكتاب وناشريه ولجميع المسلمين والمسلمات الأحياء منهم والأمـوات ..

أخوكم ::

حماد حجازي (أبو موسى) – غزة – فلسطيـــن . 18/03/2011

القسم الأول

أنظمة التشغيل وإدارتها

نبذة عن القسم ::

نظام التشغيل هو برنامج ضخم يتم تثبيته على الجهاز الشخصي بهدف تصفح الملفات وإدارة البرامج والتطبيقات المختلفة ومن أمثاله النسخ المختلفة لمايكروسوفت ويندوز (Seven , Vista , XP)،، ولينكس ،، و ماك ،، وأخيرا نظام قوقل كروم ..

سيعنى هذا القسم بكيفية تثبيت أنظمة تشغيل مايكروسوفت المختلفة ،، وسيحاول أن يوضح بالتفصيل الممل كيفية اعتماد المستخدم العادي على نفسه في صيانة برمجيه لحاسبه وتثبيت نسخ الويندوز بنفسه وقتما يريد دون الحاجة لمحلات الصيانة وذلك لعدة أسباب مهمة ::

لإغلاق بوابة قد يدخل منها الفيروسات سواء بعلم أصحاب بعض محلات الصيانة الذين يستهدفون الزبائن الذين وثقوا بهم ،، أو بدون علمهم نتيجة لجهل الكثيرين من أصحاب تلك المحلات بأسس الحماية والفحص ..

هذا بالإضافة إلى سرد الكثير من المعلومات الأولية والتي ستفيد بإذن الله المستخدم العادي في مشوار توفير الحماية الشخصية لجهازه أو أي جهاز لشخص آخــر قد يتعامل معه ..

مع معلومات نخصصها للإطلاع على أهمية التفريق بين الملفات ومواقع الإنترنت وما لذي يجب إتباعه لدرء أي مخاطر قد نواجهها .

فعلى بركة الله نبدأ أولى أقسامنا التي نتمنى من العلي القدير أن تنال الرضا من القراء الكرام ..

الدرس الأول :: تعريفات وإحصائيات

الجزء الأول :: تعريفـات

إن أهم ما يميز العلم الحديث بكافة مجالاته هو وجود العديد من الوسائل التي تسهل طرح المعلومة ووصولها لذهن المتلقي بالشكل المطلوب ،، وكان مجال التكنولوجيا هو المصدر الأضخم على مر التاريخ للمعرفة والتطوير حيث ساهمت التكنولوجيا في نقلة نوعية للمجتمعات ، ويستطيع الآن الكثير من الأفراد والمجوعات التعلم وتبادل المعلومات بشكل سريع وأكثر فائدة من قبل ، وتسارعت التطورات التكنولوجية حتى وصلت إلى اختراع الانترنت والذي يستخدمه الآن أكثر من ثلث سكان العالم ، هذا بالإضافة إلى كثرة المصادر العلمية المدفوعة والمجانية التي تيسر عمل الباحث عن المعرفة وتعطيه المعلومة على طبق من ذهب بشكل يتناسب مع سرعة العصر وتطور المعرفة المطرد .

لذا سنعتمد بإذن الله على التكنولوجيا وما توفره في مجال صناعة الشروحات وتوضيح المفاهيم ، إما بالكتابة أو بالصور والفيديو والصوت وجميع الوسائط التي تخدم الهدف في تحقيق الحماية المتكاملة إن شاء الله ..

ملاحظة مهمة هذه التعريفات تفيد المستخدم العادي فقط ، وهي مبسطة جداً ليستطيع إدراكها الجميع أما نم يبحث عن التفاصيل المعقدة فلن يجدها هنا ، لأننا نستهدف المستخدم ذو الخبرة البسيطة والذي سنوصله بإذن الله إلى التحكم الكامل بجهازه الشخصي وفحصه وتحصينه .

تعريفات مهمة في مجال الأجهزة الشخصية ::

١ – الهاردوير Hardware

هي جميع القطع المادية في الجهاز الشخصي من شاشة وكي بورد وما إلى ذلك .

٢ – السوفتوير Software

جميع البرامج والأشياء المعروضة أمامك على الشاشة ، سواء كان نظام تشغيل أو صور وملفات وما إلى ذلك .

٣ ـ قطع الكومبيوتر وأسمائها



- **الهاردسك Hard Disk**
  قطعة يتم تركيبها لحفظ المعلومات والاحتفاظ بها
  حتى لو تم قطع التيار الكهربائي ، وهو في الغالب
  يحتوي على جميع الملفات الخاصة بك .



- **الرام Ram**
  الذاكرة المؤقتة وتعرف عن المستخدم العادي
  بأنها من أهم القطع التي تؤثر على سرعة الجهاز.



- **المعالج CPU**
  هو معالج البيانات الرئيسي داخل الجهاز ، ويمثل
  أهم المكونات الداخلية فيه ، ويجب أن نختار
  الأفضل في حال فكرنا في شراء جهاز جديد .



- **اللوحة الأم Motherboard**
  هي اللوحة الرئيسي التي يتم ربطها بكافة مكونات
  الهاردوير من هارد ومعالج وغير ذلك .



- **الكروت الإضافية Cards**
  هي قطع مثل الكروت يتم تركيبها في أماكن معينة
  على اللوحة الأم حسب احتياجات المستخدم وهي
  في الغالب إضافات كمالية للمستخدمين
  وأمثله عليها كروت الديجيتال والمونتاج .. وغير ذلك.



- **مزود الطاقة Power Supply**
  هي القطعة المسئولة عن إدارة الطاقة والكهرباء
  وتوزيعها على قطع الجهاز الداخلية والخارجية .

تابع الصور التالية لمعرفة المزيد عن قطع الأجهزة والأسماء
حتى تميز وتدرك الفرق بينها ..

Mouse الماوس	**Keyboard الكي بورد**	**Monitor الشاشة**
Webcam كاميرا	**Flash Disk فلاش دسك**	**USB مدخل**
Speakers سماعات	**DVD قارئ الاسطوانات**	**Headphone**

٤ ـ أنظمة التشغيل ::

أنتجت شركة مايكروسوفت العديد من أنظمة التشغيل إلا إن الكثير من هذه الأنظمة لم يعد مستخدماً ، والمستخدم حتى الآن من قبل المستخدمين العاديين ٣ إصدارات من تلك الأنظمة وهم ويندوز اكس بي وويندوز فيستا وويندوز سيفين .

وفي بحوث مختلفة على الانترنت تؤكد شركات عملاقة أجرت العديد من التجارب على أنظمة تشغيل مايكروسوفت أن نظام ويندوز اكس بي هو الأفضل حتى الآن من نواحي كثيرة أهمها السرعة والأمن .

ولكن أنظمة مايكروسوفت ليست الوحيدة ، هناك بالإضافة إليها نسخ مختلفة من أنظمة التشغيل كـ اللينكس و الماك وقوقل كروم وهو إصدار جديد من المتوقع أن ينافس مايكروسوفت ويندوز من إنتاج شركة قوقل العملاقة .

ولكننا وفي هذه الدورة نخير المستخدم بين الثلاثة أنظمة ونترك له حرية الاختيار ، وسنطرح في دروس لاحقة مزايا وعيوب لكل نظام في جوانب أمنية .

ومع أن ويندوز اكس بي نظام قديم وتم اكتشاف العديد من الثغرات البرمجية الخطيرة فيه إلا انه مازال يستخدم بشكل كبير وذلك لأن معظم تلك الثغرات قد تم ترقيعها بشكل هائل ، وتم إنتاج آلاف البرمجيات التي تطور وتدعم هذا النظام الرائع .

ويعد ويندوز اكس بي الأفضل والأكثر شهرة لتمتعه بمزايا كثيرة أهمها دعم جميع الأجهزة الحديثة والقديمة بالإضافة إلى سلسلة هائلة من المزايا ، ومع أن ويندوز فيستا و سيفين قد جاءا بعده ولكنه وحتى اللحظة يتمتع بجمهور عريض مازال يتمسك به .

يقصد بنظام التشغيل البيئة المخصصة لإدارة الجهاز الشخصي واستخدامه ، والشركة الرائدة في هذا المجال حتى الآن تعتبر مايكروسوفت حيث أن الدورة بشكل كامل تم شرحها على إصدارات ويندوز مايكروسوفت .

جدول يوضح الفروق في القوائم بين إصدارات الويندوز المختلفة ..

Windows 2000

Block style

Continuous style

Windows XP

Block & continuous style

Marquee style

Windows Vista

Normal state

Marquee style

Paused state

Error state

Windows 7

Taskbar button

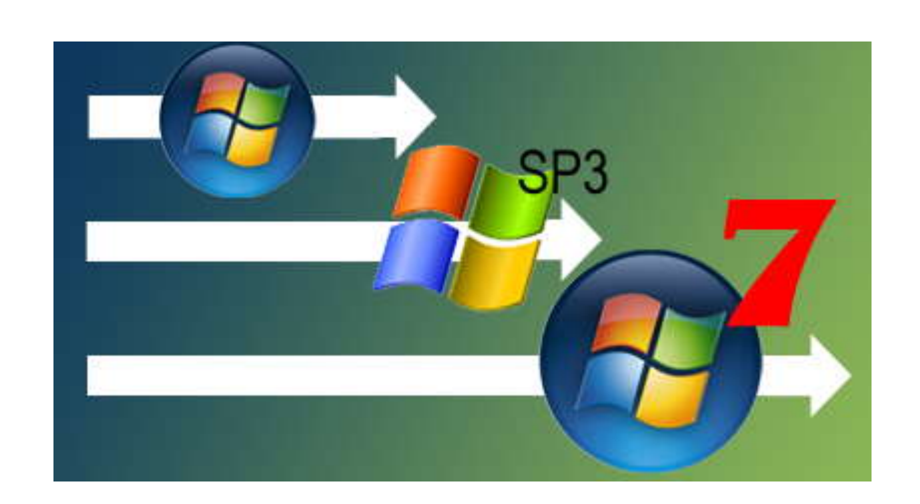
Normal state

Marquee style

Paused state

Error state

صورة توضح نتائج بعض الاختبارات وتفوق ويندوز اكسبي على فيستا



٥ ـ التعريفات ::

كـ مستخدم عادي لا يلزمك الخوض في كثير من الأمور التي لا تستلزم معرفتها إلا لفريق خبراء ومبرمجين متخصصون ، لذا ببساطة يجب أن تعلم إن الكومبيوتر يجب أن يتعرف على قطع الهاردوير المثبتة فيه ، ويعرف هذا بالتعريفات .
ولتبسيط الفكرة ففي كل مؤسسة عادية عالمية يوجد بواب يتعرف على الشخص المراد دخوله إلى تلك المؤسسة ليقوم بمهام ما .
وهذا هو دور التعريف حيث يخبر نظام التشغيل بأنه من إنتاج شركة كذا ، ووظيفته كذا وكذا ..

وتم ذكر هذا الجانب لأنه جانب مهم بعد تثبيت نظام التشغيل يجب عليك تعريف القطع التي لم يستطيع نظام التشغيل معرفتها .
وهذا من خلال أقراص قد تتوافر معك حين شراء الجهاز الشخصي ، أو من خلال اسطوانة شاملة تحتوي تعريفات معظم القطع الموجودة في السوق وسيتم شرح هذه الفكرة بالكامل بإذن الله .
وسيتم طرح شرح فيديو لاسطوانة تحتوي على موسوعة ضخمة من التعريفات لتسهل عليك إيجاد وتثبيت التعريفات . فيديو ق١ ف٣
هذا بالإضافة إلى شرح فيديو آخر لبرنامج مميز في مجال جلب التعريفات بل وتحديث الموجود لديك . ق١ ف٤

٦ ـ برامج الحماية ::

تم انتشار برامج الحماية بشكل خيالي بعد انتشار الحاسب مباشرة للشركات والأشخاص على حد سواء ، ويتنافس في مجال الحماية آلاف الشركات إلا أن المشهور منها لا يزيد عن ٤٢ برنامج حماية لأكثر من ٢ مليار مستخدم للانترنت ، وهو رقم بسيط جداً مما يظهر سيطرة هذه الشركات على هذا القطاع المربح لهم ، وقد تم نشر العديد من الفيروسات من خلال تلك الشركات على الشبكة بهدف بيع منتجاتها وتوفير الحماية من هذه الفيروسات الجديدة والتي لم يتم إنتاجها لولا اهتمام بعض الشركات بالبرمجيات الخبيثة وتطويرها المستمر بهدف الوصول إلى اكبر شريحة شرائية ، إلا أن هذه البرامج تستطيع كـ مستخدم عادي أن تستخدمها بسبب انتشار البرامج المقرصنة على الانترنت والتي تسمح لك استخدام أي برنامج دون الحاجة لشرائه .

ومن أشهر برامج الحماية ::

Avira	KaspersKy	Avast
Dr.Web	Norton	Bitdefender
McAfee	Microsoft	AVG

٦ ـ المتصفح ::

هو مستكشف الانترنت يتم نم خلاله استعراض صفحات المواقع وما قد تحتويه من صور وملفات وفلاش وغير ذلك الكثير ، ويعتبر المتصفح الداخلي مع نسخ الويندوز هو أشهر المتصفحات حتى الآن ولكنه يحتوي على الكثير من الثغرات الخطيرة والتي قد يستخدمها البعض في إلحاق الضرر لمتصفح تلك المواقع .

وفي الفترة الأخيرة بدأ الكثيرين يحولون اهتمامهم من استخدام المتصفح الملحق مع الويندوز وهو **Internet Explorer**



إلى متصفحات أخرى منافسة أهمها وأشهرها

متصفح **Mozilla Firefox**



تعتبر شركة موزيلا أهم شركة تعنى بالبرامج المفتوحة المصدر وتطورها وتضم بينها أشهر وأضخم المبرمجين العالميين الذين أخذوا على عاتقهم حماية المستخدمين وتطوير قدرات البرمجيات الحرة لتنافس الشركات التي تهدف في العديد من الخدمات التي تقدمها إلى إرضاء ذوق المشتري لا أمن المستخدم والحفاظ على معلوماته الخاصة ، وما إلى ذلك مما يضمن انترنت آمن ومجاني ومفتوح المصدر .

ومن أهم ما يميز هذا المتصفح ملايين الإضافات التي يمكن إضافتها بهدف توفير حماية متكاملة ومنع بعض المواقع من استهداف الجهاز الشخصي أو سرقة معلومات شخصية ، هذا بالإضافة إلى التطوير المستمر دون إزعاج المستخدم .

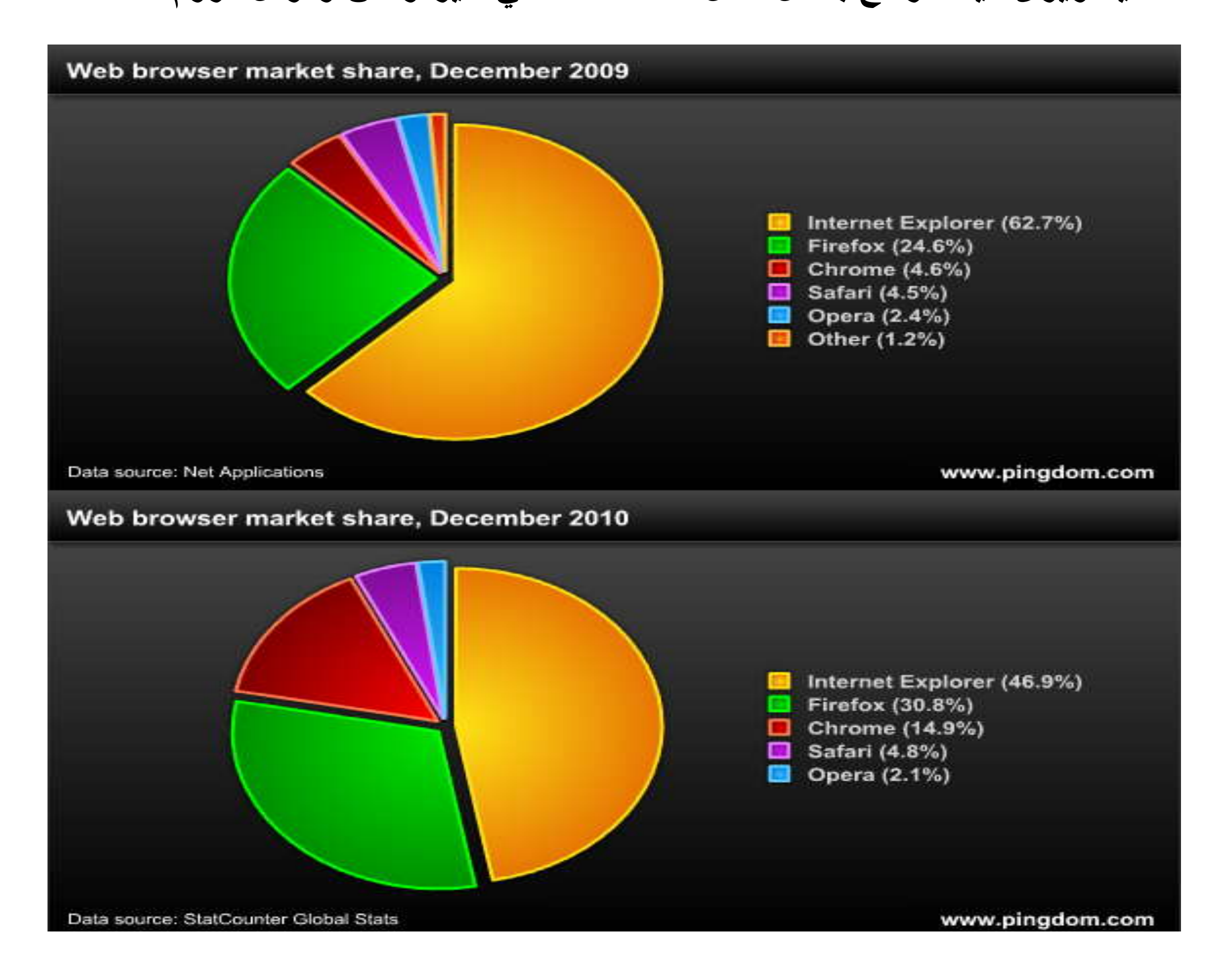
ومتصفح Google Chrome



وهو متصفح من إنتاج شركة قوقل العالمية ، وهي الشركة التي تنبأ الكثيرين بأنها ستكون الشركة رقم واحد في مجال تكنولوجيا حيث أنها الآن تسعى إلى إنتاج نظام تشغيل بخدمات كثيرة وجديدة وهو في قمة الأمان كما قالت الشركة وسيأخذ الهاكرز خصوصا أطفال الهاكرز وقتا طويلا قد يتعاملوا مع اختراق النظام الجديد لأنهم الآن في الغالب تعلموا على مدار سنوات طويلة استلزم خلالها تجول وقراءة آلاف المراجع وتجربة آلاف الطرق .

إلا إني مازلت أفضل العملاق فايرفوكس !!

ولكم حرية الاختيار فيما يناسب حاجتكم ، ومن مازال يتحير فليدقق في الاحصائيات التالية ويرى كيف ارتفع بشكل هائل عدد مستخدمي فايرفوكس وقوقل كروم



٧ - الآي بي IP ::

كل شخص في العالم عندما يرسل له رسالة يتم التعرف عليه ليس من خلال اسمه فقط ، وإنما هم شيء في الرسالة هو العنوان .
وكل شخص في الإنترنت له عنوان أيضا حتى يتم تمييزه عن غيره .
ويعتبر الآي بي الآن من أهم المعلومات الشخصية والتي يجب الانتباه إليها إذا ما دخلنا بعض المواقع أو تواصلنا عبر برامج المحادثة .
هذا فقط إذا لم نكن نستخدم أساليب حماية ستعتبر حصنا منيعاً لن يتم تجاوزها فاحرص على الاستمرار في هذا الكتاب آملين أن نقدم لك كل ما يفيدك في تحصين جهازك وحماية نفسك من المتخلفين الباحثين عن ثغرة كـ الفئران في المنازل .
فما من هدف سيكون من اقتحام جهاز مستخدم عادي إلا التجسس عليه والتلذذ في إرهابه وتخريب عالمه الصغير .

وسنتعلم بإذن الله كيفية مراقبة اتصالاتك والمعلومات الصادرة والواردة لجهازك ، وكيفية التعرف على أن الاتصالات تتم بأشخاص أو مواقع ، وتتبع لأي جهة !!
وكل هذا في الأقسام اللاحقة بإذن الله .

عنوانك على الانترنت يتم تمييزه من خلال أربع أرقام يفصل بين كل منها نقطة كما نلاحظ في السطر التالي كـ مثال فقط ::

20.100.0.50

هذا هو العنوان والحد الأقصى لكل رقم من تلك الأرقام هو 254
وتستطيع معرفة الآي بي الخاص بك عن طريق الذهاب إلى أحد هذه المواقع ::

http://www.whatismyip.com/
http://www.ipmap.com/

وغيرها الكثير الذي يقدم نفس الخدمـــة .
وهناك برامج لتغيير الآي بي حتى تتصفح بشكل خاص ، وسنشرح بعضها لاحقاً في درس خاص بالتصفح الآمن ..

٨ ـ الدوس أو موجه الأوامر MS-Dos ::

كـ مستخدم عادي لا يلزمك قراءة هذا الجزء ولكن رأيت من الواجب ان يتم الاشارة إليه فهو أول واجهة للتعامل بين المستخدم والحاسب ومازالت تستخدم في العديد من المؤسسات الأمنية في العالم والشركات وفي بعض أنظمة التشغيل على اختلاف التسمية والأوامر ..

ويتم الوصول إليه في ويندوز XP
من خلال ابدأ ثم تشغيل ثم كتابة CMD
كما في الصور التالية ::





بعدها سيظهر موجه الأوامر أو الدوس ، وتستطيع كتابة بعض الأوامر للتعرف عليه أكثر كـ مثال بسيط

Netstat –an

وهو أمر لإظهار كافة الاتصالات التي يقوم بها جهازك سواء صادرة او واردة .
وسيتم شرح عملية مراقبة هذه الاتصالات بهدف اكتشاف أي عمليات اختراق قد تحدث على الأجهزة في قسم فنون الفحص ، ويسمى هذا الفحص بالفحص اليدوي

لا تقلق كثيراً فهناك مئات البرامج التي سيتم ادراجها وستسهل عليك القيام بهذا الأمر .

٩ – الفيروس ::

هو ملف يحتوي أكواد برمجية قد تلحق الضرر بجهازك ، وقد تنسخ نفسها بنفسها ، أو تحاول التخفي وإزالة بعض أدوات ويندوز الموجودة داخله أو قد تستخدم الفيروسات بعض الشركات في عرض إعلانات معينة مصنعة لبرامج تدعي أنها تطهر جهازك من الفيروسات وهي في الغالب من صناعة شركات وليس أفراد عاديين .

ولكن لم يتم منذ ظهور هذه الفيروسات اتهام أي من الشركات العملاقة بصناعة أي برمجية خبيثة ، لأن هذه الشركات تربطها علاقات شراكة بالكثير من الحكومات والمؤسسات الأمنية في العالم ، ويتم دعمها من خلال قطاع واسع يسيطر على مجال الاتصالات وأمن المعلومات والبنوك وغير ذلك الكثير .

وفي الغالب يتم ربط إنشاء الفيروسات ونشرها بشخص مجنون أو مريض نفسي يتم القبض عليه وصنع بعض البرمجيات التي تطهر الفيروس من شركات برامج الحماية وسواء ترفق هذه الإضافات داخل البرنامج الرئيسي أو تصدر إضافة معينة تقوم بحذف فيروس أو مجموعة فيروسات غالبا ما يتم توزيعها مجاناً بهدف الإعلان للأشخاص المترديين في شراء مكافح فيروسات إننا الشركة الأقوى وما إلى ذلك ، ويرجع البعض سرعة انتشار الفيروسات إلى الانترنت حيث يتم انتقال الفيروس سريعاً من خلال المواقع والزوار والبريد الالكتروني ووسائل التواصل .

أنواع الفيروسات ::

الدودة

أكثر الفيروسات انتشارا كانت فيروسات عبارة عن ديدان تلتصق بالبرامج الحميدة بهدف إلحاق الضرر بأكبر قطاع ممكن من الأشخاص ، وبالإضافة إلى ذلك تنسخ نفسها تلقائيا في أجهزة كـ الفلاش دسك والاسطوانات وترسل نفسها تلقائيا لأكبر عدد من الأجهزة على شبكة الجهاز المصاب .

تروجان Trojan Horse :

من أكثر أنواع الفيروسات شراسة ، وهو موجه لأمور التجسس فلن يضر جهازك إطلاقاً بل لن تلاحظ أساسا وجود أي فيروس او أي شيء غير مرغوب فيه ، وسيستمر جهازك بإرسال معلوماته وعنوانه الجديد في كل مرة تتصل فيها

بالانترنت ، وتتم صناعته للتحكم بالجهاز المستهدف ، وقد تتم العملية بشكل عشوائي إذا يتم دمج دودة تسعى لنشر التروجان مع عدم تفعيل خواص الضرر الظاهرية فيها ، وهي أكثر تكنولوجيا مستخدمة الآن من قبل أطفال الهاكرز .

١٠ ـ مصطلح أطفال الهاكرز ::

هو مصطلح تم إطلاقه عربيا بهدف الفصل بين الهاكرز ذوي الخبرات البرمجية العالية أما الهاكرز الهاوي الذين تتلمذوا على يد هاكرز جلبوا بعض المعلومات من مصدر أو آخر ، وأنشئوا المنتديات بهدف تعليم الأشخاص اختراق الأجهزة ، والناظر لحال المنتديات العربية المتخصصة في هذا الجانب يكاد يجزم أن هذه المنتديات مخصصة للاختراق ولا تحوي في الغالب أي شروحات عن كيفية الحماية الصحيحة من الألف إلى الياء ، فتجد فيها دورات من الصفر لكيفية الاختراق ووصول الضحايا (الأجهزة المخترقة) إلى جهاز الهاكرز المولود على أيديهم ، وكل هذا بهدف اختراق الأصل وما يترتب عليه ، بمعنى انه في الغالب يتم تعليم بعض الجنود الجدد الذين سيريحون الكبار وسيعطونهم ما يريدونه على طبق من ذهب .

المعلومة المطلوبة قد تكون صور أو فيديو لأشخاص بشكل عشوائي يتم جمعها وبيعها على جهات أو مؤسسات حقيرة تسعى لنشر الفضائح وتحويل المجتمع العربي وتفكيره من مجتمع يبحث عن العلم ويعلوا في هذا المجال المشرف ، ويصبح له شأن بين دول تقول أن من لا يفهم لغة التكنولوجيا فهو أمي .!!!

إلا أن الكثيرين من الدارسين لهذا العلم ، وللأسف الشديد يكون الهدف متشابه للمعلم حتى لو لم يظهر ، وتتراكم المعلومات عليه حتى يتمكن فعلا من الاختراق وطبعا سيجرب وأول ما يجرب نجاح هذه العملية في أكثر الناس قرابة أو ثقة ، ثم يتوسع في المنتديات المحيطة ويتعلم أساليب بسيطة في الدمج واستغلال نقاط ضعف المستخدمين ، بل ويكتشف هذا الطفل الوليد أن أغلب أساليبه المستخدمة الآن كان يستخدمها غيره معه ، ونجحت فيجرب ويجرب ولن يتم إشباع رغباته ، لأنه وكل ما يتمكن من اختراق جهاز يجد المزيد والمزيـــد ..

سنتعلم بإذن الله ،

كيف نحمي أنفسنا من الجميـع سواء كان قريباً ..

أم بعيـداً .

وستميز منذ الآن ما تريد وما ترفض ،

وستفحص هل خذلك صديق أم أخ ، أم حاول حمايتـك طبقاً للواجب والأمانة ..

وفق الله كل من يريد تغيير الأمة للأفضل ،

وحسبنا الله ونعم الوكيل في كل من يسعى لفضيحة إخوانه وأخواته ،

في الحديث الصحيح رواه مسلم عن أبي هريرة -رضي الله عنه- عن النبي – عليه الصلاة والسلام- أنه قال: (من نفس عن مؤمن كربة من كرب الدنيا نفس الله عنه كربة من كرب يوم القيامة، ومن يسر على معسر يسر الله عليه في الدنيا والآخرة، ومن ستر مسلما ستره الله في الدنيا والآخرة)

قصة من صفحات الإنترنت ::

قال أحمد بن مهدي: جاءتني امرأة ببغداد، ليلة من الليالي، فذكرت أنها من بنات الناس، وقالت: أسألك بالله أن تسترني، فقلت: وما محنتك؟!، قالت أكرهت على نفسي وأنا الآن حامل، وبما أنني أتوقع منك الخير والمعروف، فقد ذكرت لكل من يعرفني أنك زوجي، وأن ما بي من حمل إنما هو منك فأرجوك لا تفضحني، استرني سترك الله عز وجل.

سمعت كلامها وسكت عنها، ثم مضت. وبعد فترة وضعت مولوداً، وإذا بي أتفاجأ بإمام المسجد يأتي إلى داري ومعه مجموعة من الجيران يهنئونني ويباركون لي بالمولود. فأظهرت لهم الفرح والتهلل، ودخلت حجرتي وأتيت بمائة درهم وأعطيتها للإمام قائلا: أنت تعرف أنني قد طلقت تلك المرأة، غير أنني ملزم بالنفقة على المولود، وهذه المائة أرجوك أن تعطيها للأم لكي تصرف على ابنها، هي عادة سوف أتكفل بها مع مطلع كل شهر وأنتم شهود على ذلك ..واستمررت على هذا المنوال بدون أن أرى المرأة ومولودها. وبعدما يقارب من عامين توفي المولود، فجاءني الناس يعزونني، فكنت اظهر لهم التسليم بقضاء الله وقدره، ويعلم الله أن حزناً عظيماً قد تملكني لأنني تخيلت المصيبة التي حلت بتلك الأم المنكوبة. وفي ليلة من الليالي، وإذا بباب داري يقرع، وعندما فتحت الباب، إذا بي أتفاجأ بتلك المرأة ومعها صرة ممتلئة بالدراهم، وقالت لي وهي تبكي: هذه هي الدراهم التي كنت تبعثها لي كل شهر مع إمام المسجد، سترك الله كما سترتني.حاولت أن أرجعها لها غير أنها رفضت، ومضت في حال سبيلها. وما هي إلاّ سنة وإذا بها تتزوج من رجل مقتدر وصاحب فضل، أشركني معه في تجارته وفتح الله عليّ بعدها أبواب الرزق من حيث لا أحتسب.

"وَلَقَدْ خَلَقْنَا الْإِنسَانَ وَنَعْلَمُ مَا تُوَسْوِسُ بِهِ نَفْسُهُ وَنَحْنُ أَقْرَبُ إِلَيْهِ مِنْ حَبْلِ الْوَرِيدِ (١٦) إِذْ يَتَلَقَّى الْمُتَلَقِّيَانِ عَنِ الْيَمِينِ وَعَنِ الشِّمَالِ قَعِيدٌ (١٧) مَا يَلْفِظُ مِن قَوْلٍ إِلَّا لَدَيْهِ رَقِيبٌ عَتِيدٌ وَجَاءتْ سَكْرَةُ الْمَوْتِ بِالْحَقِّ ذَلِكَ مَا كُنتَ مِنْهُ تَحِيدُ (١٩) وَنُفِخَ فِي الصُّورِ ذَلِكَ يَوْمُ الْوَعِيدِ (٢٠) وَجَاءتْ كُلُّ نَفْسٍ مَّعَهَا سَائِقٌ وَشَهِيدٌ (٢١) لَقَدْ كُنتَ فِي غَفْلَةٍ مِّنْ هَذَا فَكَشَفْنَا عَنكَ غِطَاءكَ فَبَصَرُكَ الْيَوْمَ حَدِيدٌ وَقَالَ قَرِينُهُ هَذَا مَا لَدَيَّ عَتِيدٌ (٢٣) أَلْقِيَا فِي جَهَنَّمَ كُلَّ كَفَّارٍ عَنِيدٍ (24)مَّنَّاعٍ لِّلْخَيْرِ مُعْتَدٍ مُّرِيبٍ"

١١ – البوت نت BotNet ::

البوت نت هي تقنية يتم استخدامها للتحكم في عدد هائل من الضحايا بكود برمجي واحد ، أو بأوامر موحدة لجميع الأجهزة المصابة .

أكثر تقنية ترعب المؤسسات والشركات في الوقت الحالي ، ولكنها لا تستهدف الشركات الآن ، بل تستهدف الأشخاص الذين وللأسف يفتقرون أسس الحماية الصحيحة والتي تمكنهم من تحصين أجهزتهم ومنع تطفل أي من هذه البرمجيات الضارة ، تم تصميم البوت نت في أوائل القرن الحالي إلا أنه لم يكن مع الأشخاص العاديين بل كان يتم التحكم به وتطويره من قبل المافيا العالمية أو مؤسسات وشركات عالمية ، هدفها نشر فكر الرعب والحاجة للحماية أو استهداف الشركات التي كانت تتكبد خسائر مالية ضخمة جراء الثغرات الأمنية في أنظمتهم ، والتي في الغالب تم تصميمها من قبل هاكرز منشقين استخدموا معرفتهم في هذه الشبكة أو تلك وباعوها لمن يريد الانتقام أو لأي هدف آخر ..

حاليا البوت نت وصل إلى أيدي بعض الهاكرز والذين يستخدمونه في اختراق مئات أو آلاف الأجهزة ، وفي الغالب يتم التحكم بالضحايا من قبل أكثر من جهة ، بمعنى أن الانترنت يتم إدارته من شركات عملاقة بالأصل وهؤلاء مدراء البوت نت (BotMasters) هم مسهلي عمل من يستهدف الأشخاص ويجمع الإحصائيات المختلفة ، وأكبر بوت نت تم اكتشافه كان يبلغ عدد الضحايا فيه إلى أكثر من

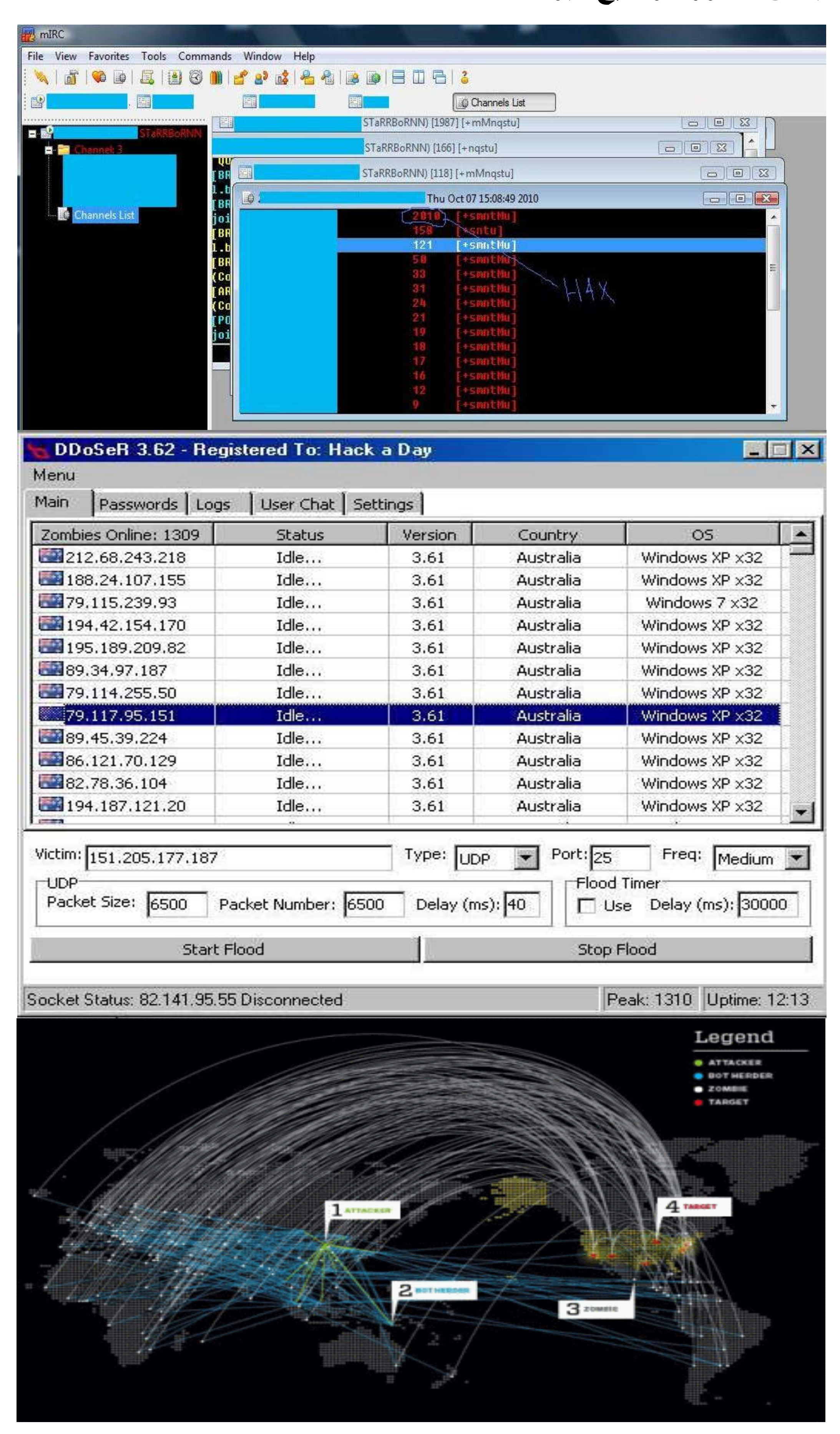
825 ألف جهاز ، وهو رقم ضخم جداً بالطبع .

أهداف إنشاء البوت نت :

في البداية كانت هجمات البوت نت في الغالب تحدث نتائج مدمرة ، قد تسبب انهيار الأنظمة ، أو التجسس أو فتح ثغرات كبيرة في الأنظمة المستهدفة لدخول جيش من الهاكرز لسرقة معلومات هامة أو القيام بأمور أخرى داخل النظام بتكليف طبعا من الغير ، إلا أن البوت نت الآن لا يعدو كونه لعبه بيد بعض الهاكرز لإشغالهم وإلهائهم في برمجية ماتت ، ذلك لأن خروجه للمستخدم العادي ينذر أن هناك شيء أضخم وأفضل تم إنتاجه فعلياً .

البوت نت يتم دمج كثير من الأساليب داخله لمحاولة الاختراق الآلي ، بمعنى أن جهاز الضحية سيكون عبارة عن باحث ضخم للبوت الأساسي بهدف انتشار البوت في اكبر عدد ممكن ، ويتميز كل بوت عن آخر بهذه الخاصية بالذات .

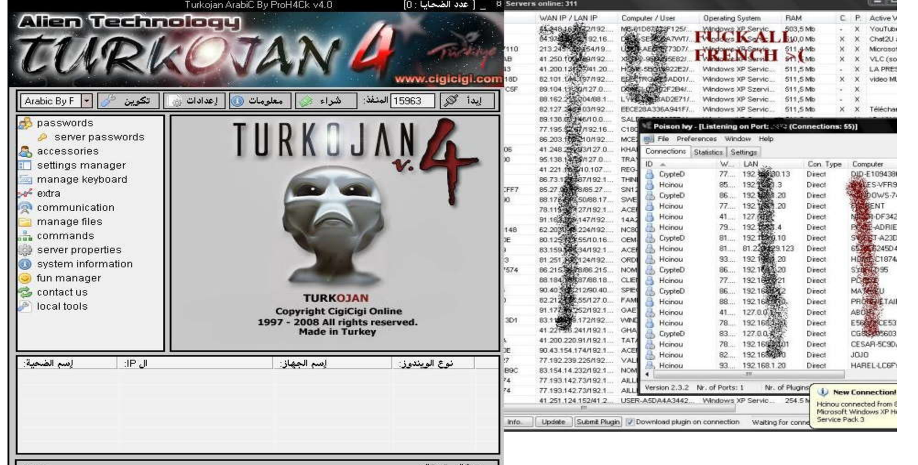
بعض الصور لتوضيح البوت نت ::



برنامج يتم استخدامه من قبل الهاكرز لإدارة الضحية ، وغالبا يحتوي هذا البرنامج على كثير من الإمكانيات التي تطبق التحكم على جهاز الضحية (الشخص المخترق)

وهناك الكثير من برامج الاختراق التي يتم استخدامها بشكل كبير ، ولكن خبراء الهاكرز يستخدمون برامج خاصة بهم تم إنشائها على أيديهم بهدف سهولة تشفيرها من برامج الحماية المشهورة والتي قد تتواجد في أجهزة الضحايا .

الهاكرز العرب يستخدمون هذه البرامج والتي سيتم شرحها ، وشرح غيرها خلال هذه الدورة ..



Bifrost

Poison Ivy Rat

Turkojan

SpyNet

Cerberus

وغير ذلك هناك برامج تظهر وتختفي ، وهي في الغالب من إنتاج الغرب الكافر ، بهدف السيطرة على العقول العربية ، والحقيقي فقط أن أطفال الغرب لا يستخدمون هذه البرامج إطلاقا بل يبدءوا من عشق البرمجة وتطوير البرامج الخاصة والتي يستخدمونها في السيطرة على أجهزة بعضهم البعض في منافسات شريفة وتحديات يتم دعمها من الحكومات والمجال المدرسية ، والآباء وغير ذلك ،ويتم دعم الأطفال المتميزين ، وتوفير الإمكانيات المناسبة لهم لتطوير مهاراتهم !!.

بينما يتم القبض على المبرمجين العرب بهدف حماية المستخدمين ممن قد يضرهم ، وهو في الغالب لا يحدث إلا من !!!

نتمنى أن تكملوا الدورة ، وإن كنت أب أو أخ أو صديق لشخص يريد أن يتعلم وتمتلك المساعدة التي قد يحتاجها ذلك الشخص ، فباشر في مساعدته ليكتب لك الأجر ، وتذكر أنك ستسأل عن كل شيء ..

تقديري واحترامي لجهود الجميع ..

١٣ ـ الباتش أو سيرفر برامج الاختراق Server ::

هو برنامج صغير يتم إرساله في الغالب مع برنامج آخر بشكل متخفي ، ويتم دمجه في البرامج الحميدة أو في صور أو فيديو أو أي شيء لأنه وعند تشغيل لا يظهر أي شيء غريب للمستخدم ، ويستمر هكذا ليتيح للهاكرز إنهاء عمله دون علم الجهاز المستهدف ، وفي كل مرة يقوم الضحية بالدخول للإنترنت يرسل هذا السيرفر معلوماته للهاكرز الذي يديره ، وتعتبر هذه العملية أخطر عمليات الاختراق لأنها تهدف إلى التجسس والتجسس فقط ، فيستطيع الهاكرز حينها فعل هذه الأشياء التالية في الجهاز الذي تم استهدافه ::

١ ــ يستطيع المخترق رؤية وتحميل وتعديل وحذف جميع ملفاتك ..
٢ ــ يستطيع رؤية جميع كلمات المرور الخاصة بك ..
٣ ــ يستطيع مشاهدة ما تفعل على جهازك بشكل مباشر..
٤ ــ يستطيع تخزين كل كلمة يتم كتابتها على الكيبورد ..
٥ ــ يستطيع فتح الكاميرا..
٦ ــ يستطيع سماع الصوت ..
٧ ــ يستطيع اختراق جميع من يتعامل مع جهازك من خلال الشبكة الخاصة أو الفلاشات أو عبر برامج المحادثة ..
٨ ــ يستطيع استخدام جهازك في اختراق المواقع ..

أتمنى أن ندرك هذه الأخطار ونسعى لتحفيز غيرنا ليتعلم أمن معلوماته وجهازه ، فقد تكون أنت لا تهتم إذا ما تم اختراق جهازك ، ولكن أوليس تتعامل مع أشخاص يثقوا بك ، وأجهزتهم قد تشكل صيداً ضخما لهؤلاء الهاكرز ، تخيل معي التالي :

دخل الهاكرز لجهازك عن طريق إرسال ملف ما لك ،

ثم أخذ الايميل الخاص بك ، وأرسل السيرفر على شكل صورة أو أي برنامج حميد لبعض المضافين لديك في قائمة الايميل كـ الإخوة والأخوات والأقارب والأصدقاء والذين بالتأكيد لا تتمنى تعرضهم لأي مصاب .!!!

تم شرح ما سبق في الجزء الأول من الدرس ق١ ف١

همســة :: لا تكون بوابة الشر ، واحرص على أن تكون حصنا منيعاً بدل أن تصبح ممرا آمنا للهاكرز لاستهداف من يخصونك ..

الجزء الثاني :: إحصائيات مهمة ::

وسائل التكنولوجيا وفرت لنا تحليلا دقيقا لا يقبل الخطأ ، ووفرت لنا استخلاص نتائج من مئات آلاف عمليات الحصر والإحصاء العلمي .

وسنطرح إحصائيات لعام 2009 وعام 2010 وذلك حتى نقارن تسارع انتشار الانترنت وازدياد أعداد المستخدمين ، وفهم ما يحدث حولنا . فلنرى ::

Number of: Spam emails Email users Computer viruses Internet users Watched videos Websites Blogs Emails sent Hosted images Domain names in 2009

Email

- 90 trillion – **The number of emails sent on the Internet in 2009.**
- الترجمة : **عدد الرسائل التي تم إرسالها**
- 247 billion – **Average number of email messages per day.**
- **عدد الرسائل التقريبي لكل يوم**
- 200 billion – **The number of spam emails per day (assuming 81% are spam).عدد الرسائل الضارة في اليوم وما نسبته من الرسائل المرسلة**

Websites

- 234 million – **The number of websites as of 2009**
- عدد مواقع الانترنت

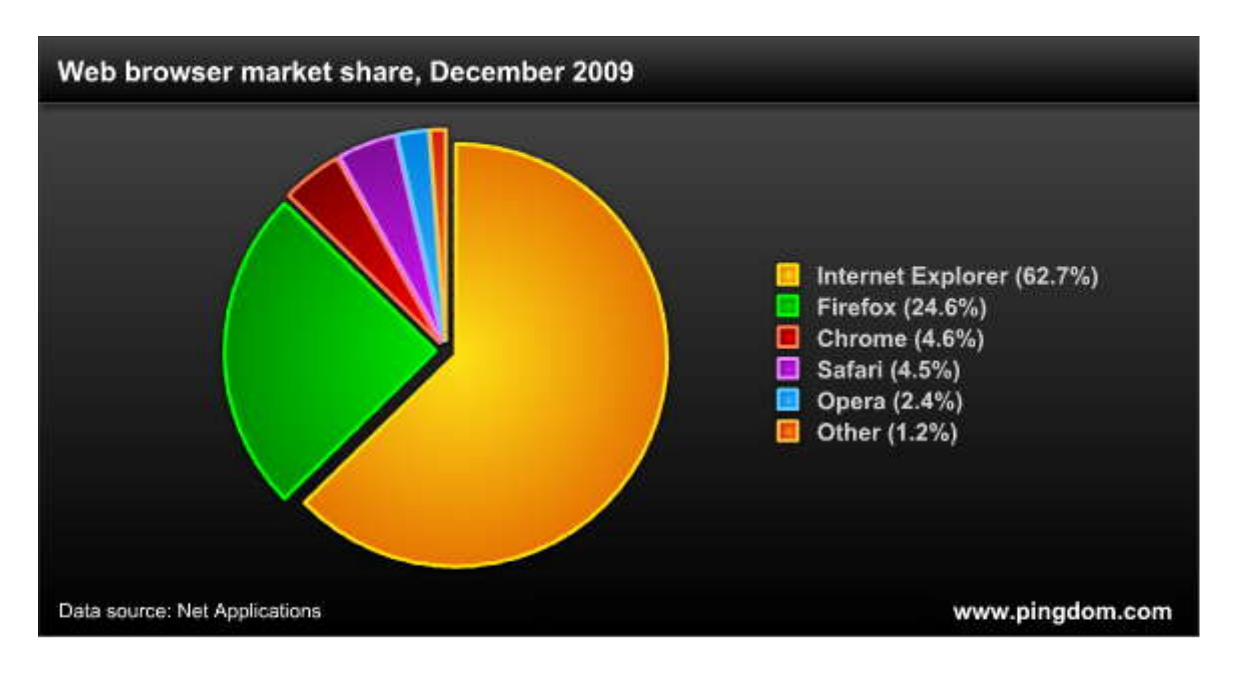
Social media

- 126 million – **The number of blogs on the Internet (as tracked by BlogPulse).عدد المدونات في الإنترنت**
- 84% – **Percent of social network sites with more women than men.نسبة النساء مقارنة بالرجال طبعا النسبة معكوسة عندنا**
- 350 million – **People on Facebook.عدد حسابات الفيس بوك**

Videos

- 1 billion – **The total number of videos YouTube serves in one day.عدد الفيديوهات التي يتم مشاهدتها يومياً**
- 82% – **Percentage of Internet users that view videos online (USA).نسبة من يشاهدون الفيديو اونلاين في أمريكا**

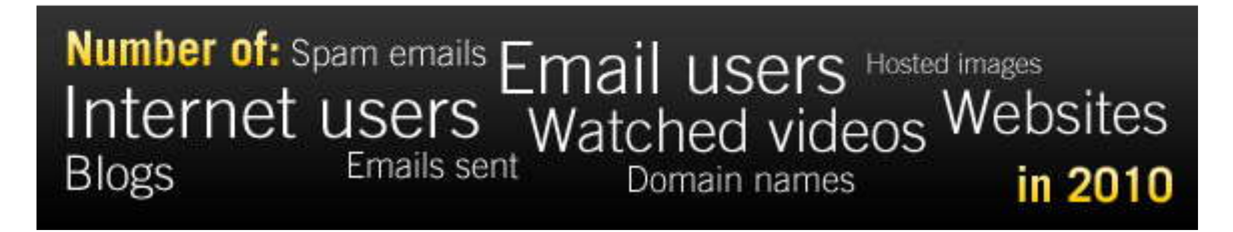
Web browsers .. نسبة مستخدمي برامج التصفح العالمية



Malicious software البرمجيات الضارة

- 148,000 – **New zombie computers created per day (used in botnets for sending spam, etc.)**
- **كل يوم يتم تجنيد هذا العدد من الاجهزة في البوت نت**
- 2.6 million – **Amount of malicious code threats at the start of 2009 (viruses, trojans, etc.)**
- **عدد الفيروسات التي أنشئت**
- 921,143 – **The number of new malicious code signatures added by Symantec in Q4 2009.**
- **عدد توقيعات الفيروسات المكتشفة من قبل شركة نورتون فقط**

[Internet 2010 in numbers]



Email

- **107 trillion – The number of emails sent on the Internet in 2010.**
- **294 billion – Average number of email messages per day.**
- **1.88 billion – The number of email users worldwide.**
- **480 million – New email users since the year before.**

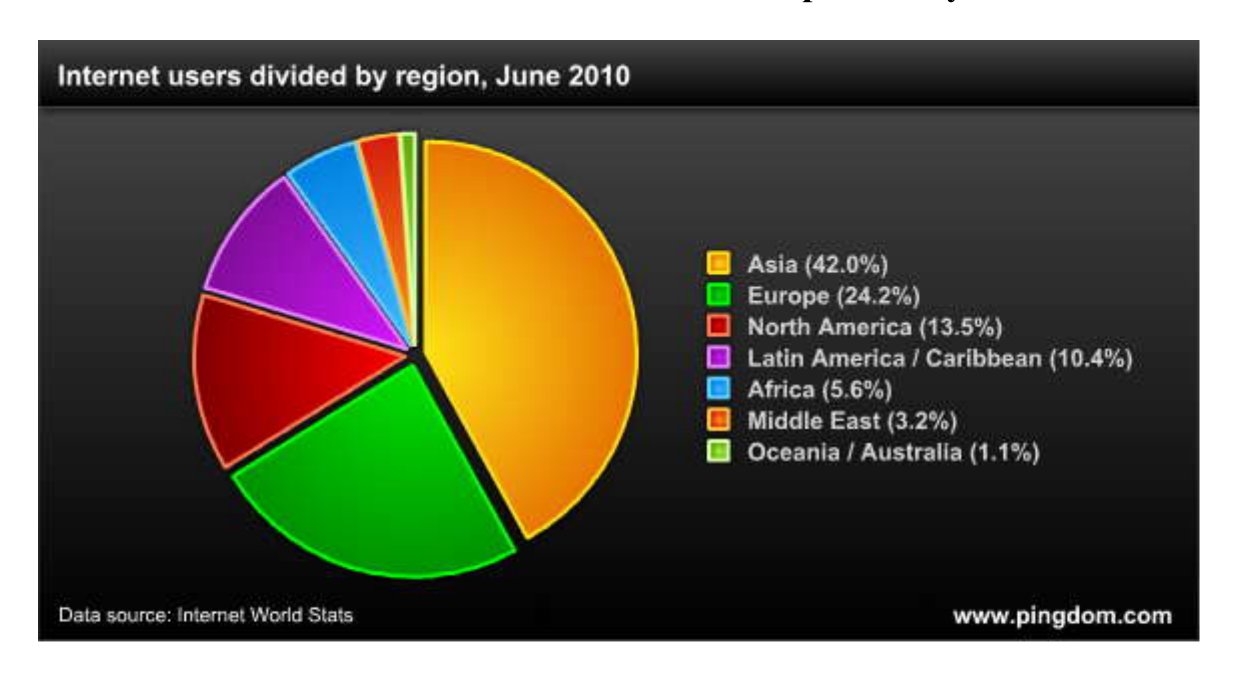
- 89.1% – The share of emails that were spam.
- 262 billion – The number of spam emails per day (assuming 89% are spam).
- 2.9 billion – The number of email accounts worldwide.
- 25% – Share of email accounts that are corporate.

Websites

- 255 million – The number of websites as of December 2010.
- 21.4 million – Added websites in 2010.

Internet users

- 1.97 billion – Internet users worldwide (June 2010).
- 14% – Increase in Internet users since the previous year.



Social media

- 152 million – The number of blogs on the Internet (as tracked by Blog Pulse).
- 25 billion – Number of sent tweets on Twitter in 2010
- 100 million – New accounts added on Twitter in 2010
- 175 million – People on Twitter as of September 2010
- 600 million – People on Facebook at the end of 2010.
- 250 million – New people on Facebook in 2010.
- 30 billion – Pieces of content (links, notes, photos, etc.) shared on Facebook per month.
- 70% – Share of Facebook's user base located outside the United States.

Videos

- 2 billion – The number of videos watched per day on YouTube.
- 35 – Hours of video uploaded to YouTube every minute.
- 186 – The number of online videos the average Internet user watches in a month (USA).
- 84% – Share of Internet users that view videos online (USA).
- 14% – Share of Internet users that have uploaded videos online (USA).
- 2+ billion – The number of videos watched per month on Facebook.
- 20 million – Videos uploaded to Facebook per month.

Images

- 5 billion – Photos hosted by Flickr (September 2010).
- 3000+ – Photos uploaded per minute to Flickr.
- 130 million – At the above rate, the number of photos uploaded per month to Flickr.
- 3+ billion – Photos uploaded per month to Facebook.
- 36 billion – At the current rate, the number of photos uploaded to Facebook per year

كانت هذه الأرقام التي يجب عليك كـ مستخدم للإنترنت الإطلاع عليها والتمعن فيها ، ونصيب العرب منها قليل جدا في كل المستويات ، بل يكاد يجزم بعض رجال الإحصاء العرب أن الدول العربية مجتمعة لا تتعدى نسبة الاستخدام لتركيا أو إيران ..!!

إن شاء الله يزداد من يبحر في عالم الانترنت من العرب ، ولكن يعرف كيفية تحضير سفينته جيداً حتى لا يغرق في هذا البحر العاصف والذي يحوي الكثير من آكلي لحوم البشر من فصيلته قبل فصائل أعداؤه ، ومن بني إخوته المسلمين قبل غيرهم من باقي الأديان ..

تقديري للجميـــع ،

ودائما نتمنى أن يكون الجيل الذي نحن فيه هو جيل الصحوة والتغيير ، ولا ننتظر الكثير لكي نغير ، دائما ما يخرج علينا الكثير من المفكرين ويقولون فلنستهدف الجيل الصغير ، الجيل الصغير هو من يجب تحضيره ، وهذه أعتبرها دعوة للإحباط ، فلماذا لا نكون نحن من نقود عملية التغيير والصحوة ، ولماذا وفينا الكثيرين ممن يستطيعون فعل أشياء عظيمة في سبات عميق ، متلهفين للسفر للخارج ، غير عابئين بأنهم سوف يسألون هل حاولتم ، أم هربتم ..

الدرس الثاني :: تثبيت نظام

ويندوز إكس بي Windows XP

نظام التشغيل ويندوز اكس بي ، أكثر الأنظمة ثباتا وسرعة حتى الآن ، وقد تم اكتشاف أغلب الثغرات وترقيعها ، وتقريبا فهم النظام الكثير ممن لم يتخصصوا في مجال الكومبيوتر لأنه نظام للمستخدم العادي ، سهل وبسيط وعليه مازال يتم دعمه نم الشركة الأم ، هذا بالإضافة إلى أن أكثر البرامج المشهورة يجب أن تدعم ويندوز اكس بي وإلا فلتترقب الفشل ، وفي إحصائيات حديثة جداً نرى أن ويندوز اكس بي مازال يتربع على عرض إصدارات أنظمة التشغيل المختلفة .

Windows XP is the most popular operating system. The Windows family counts for almost 90%:

2011	Win7	Vista	Win2003	WinXP	W2000	Linux	Mac
January	31.1%	8.6%	1.0%	45.3%	0.2%	5.0%	7.8%
2010	**Win7**	**Vista**	**Win2003**	**WinXP**	**W2000**	**Linux**	**Mac**
December	29.1%	8.9%	1.1%	47.2%	0.2%	5.0%	7.3%
November	28.5%	9.5%	1.1%	47.0%	0.2%	5.0%	7.7%
October	26.8%	9.9%	1.1%	48.9%	0.3%	4.7%	7.6%
September	24.3%	10.0%	1.1%	51.7%	0.3%	4.6%	7.2%
August	22.3%	10.5%	1.3%	53.1%	0.4%	4.9%	6.7%
July	20.6%	10.9%	1.3%	54.6%	0.4%	4.8%	6.5%
June	19.8%	11.7%	1.3%	54.6%	0.4%	4.8%	6.8%
May	18.9%	12.4%	1.3%	55.3%	0.4%	4.5%	6.7%
April	16.7%	13.2%	1.3%	56.1%	0.5%	4.5%	7.1%
March	14.7%	13.7%	1.4%	57.8%	0.5%	4.5%	6.9%
February	13.0%	14.4%	1.4%	58.4%	0.6%	4.6%	7.1%
January	11.3%	15.4%	1.4%	59.4%	0.6%	4.6%	6.8%
2009	**Win7**	**Vista**	**Win2003**	**WinXP**	**W2000**	**Linux**	**Mac**
December	9.0%	16.0%	1.4%	61.6%	0.6%	4.5%	6.5%
November	6.7%	17.5%	1.4%	62.2%	0.7%	4.3%	6.7%
October	4.4%	18.6%	1.5%	63.3%	0.7%	4.2%	6.8%
September	3.2%	18.3%	1.5%	65.2%	0.8%	4.1%	6.5%
August	2.5%	18.1%	1.6%	66.2%	0.9%	4.2%	6.1%
July	1.9%	17.7%	1.7%	67.1%	1.0%	4.3%	6.0%
June	1.6%	18.3%	1.7%	66.9%	1.0%	4.2%	5.9%

جدول يوضح بأن المعجبين ما إن ينخفضوا حتى يعودوا للارتفاع مرة أخرى ، لأنه ويندوز راقي ورائع ، ونظام مميز قد حل العديد من المشكلات الأمنية ، وتم تصميمه باحترافية عالية ، وكان إصداراً يمثل صيحة تكنولوجية من العيار الثقيل ، وما الإحصائيات إلا تؤكد أنها مستمرة حتى الآن ..

ويعتبر ويندوز اكسبي وكما تقول الإحصائيات مرغوب من ٩٠% من العائلات في العالم !!

وعليه فإن الدورة سترتكز على إغلاق ثغرات هذا النظام العملاق ، ومحاولة الاستفادة من عمره الطويل واستكشاف مميزاته ، والتي سنحاول معاً استطلاعها ، والبناء عليها وسنستخدم في هذا برمجيات تسهل القيام بكل هذا الأمر ، وستحس بعد انتهاء الدورة بإذن الله من أنك مؤهل لإدارة جهازك وأجهزة الحي بالكامل :)

تابع كيف يتم تثبيت هذا النظام الرائع من البداية ، وبالتفصيل الواضح لا الممل !!

يجب أن تحمل أولاً إصدار ويندوز XP من أحد المواقع المشهورة والتي تثق فيها ، عربيا يوجد الكثير من تلك المواقع إلا أنها تطرح وللأسف الشديد نسخ معدلة أكثر من الأصلية ، أو تقوم بشراء اسطوانة النظام من أي محل بجوار منطقتك ، وتأكد أنك تشتريها من مصدر موثوق لأن الاسطوانة قد تحتوي برمجيات تضرك من البداية ، المهم أنك ستحصل في النهاية على اسطوانة تحتوي النظام ، ولك الخيار في كيفية حصولك عليها :)

تأكد من أنك لا تريد أي ملفات من سطح المكتب أو المستندات أو المفضلة ، لأنه سيتم تهيئة النظام الحالي ، على فكرة هناك عشرات الشروحات على الانترنت التي توضح هذه العلمية ..

بعد ذلك نعيد تشغيل الجهاز ، ونضغط فور إقلاع الجهاز زر Del + F2 بشكل متقطع ، وذلك للدخول على تطبيق البيوس لتغيير السواقة التي يقلع منها الجهاز ،

وستفهم هذا لاحقاً ،، ووضعنا Del + F2 لأن بعض لوحات الأم قد تدخل الى البيوس بواسطة زر الديليت ولكن هناك من يدخل إلى البيوس بواسطة F2



بعدها سيفتح أمامك البرنامج الخاص للتحكم في الجهاز بشكل شامل ، وأرجو أن تقوم بالحذر من تعديل أي شيء إلا ما سنذكره الآن .

وهذا شرح رائع بالإنجليزي لهذه العملية والفرق بين **Bios Setup Utility** لبعض الشركات المشهورة ..

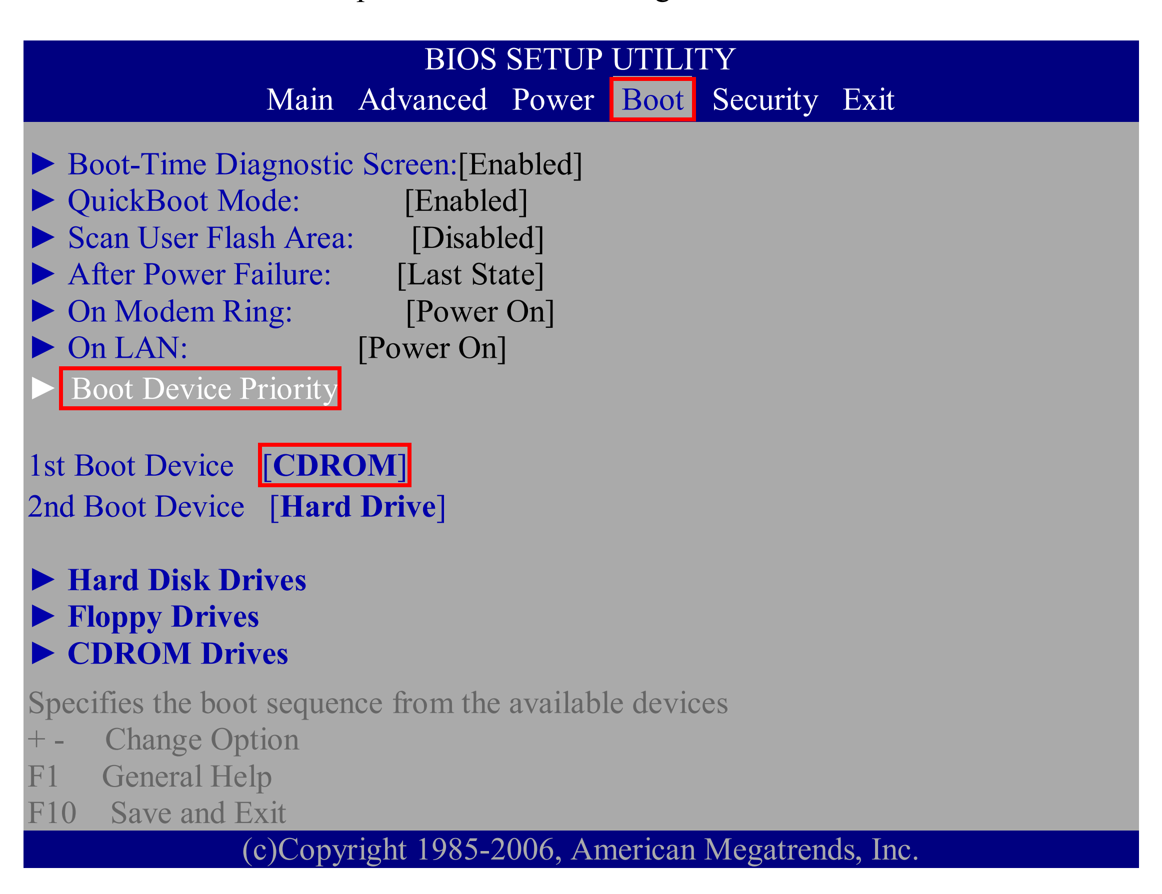
This AmiBios Require you to press DEL key to enter setup

AMIBIOS(C)2006 American Megatrends, Inc.
BIOS Date: 03/02/06 20:15:54 Ver: 09.00.07

Press DEL to run Setup

Checking NVRAM..

now you will see some similar screen and choose the BOOT option and choose Boot Device Priority and choose first boot device to **CDROM** and second boot device to **HARD DRIVE** You can press F10 to save settings.



On Award Bios you will see some similar screen and choose the right key to Enter setup

Award Modular BIOS v4.51PG, An Energy Star Ally
Copyright (C) 1984-98, Award Software, Inc.

ASUS P2B-DS ACPI BIOS Revision 1012B

Pentium III 650Mhz **Processor**
Memory Test : 262144K OK

Press DEL to run Setup
08/05/00-i440BX-P2B-DS

Now choose Advanced Bios Features

Phoenix - AwardBIOS CMOS Setup Utility

> Standard CMOS Features

> Advanced BIOS Features

> Advanced Chipset Features

> Integrated Peripherals

> Power Management Setup

> PnP/PCI Configurations

> **PC Health** Status

Frequency/Voltage Control

Load Fail-Safe Defaults

Load Optimized Defaults

Set Supervisor Password

Set User Password

Save & Exit Setup

and set First Boot Device to CDROM and Second or third to HDD-0 and Press F10 to save it.

Phoenix - AwardBIOS CMOS Setup Utility

Virus Warning
CPU Internal Cache
External Cache
CPU L2 Cache ECC Checking
Processor Number Feature
Quick Power On Self Test
First Boot Device
Second Boot Device
Third Boot Device
Boot Other Device
Swap Floppy Drive
Boot Up NumLock Status
Gate A20 Option
Ata 66/100 IDE Cable Msg.
Typematic Rate Setting
Security Option
OS Select For DRAM > 64MB
[Disabled]
[Enabled]
[Enabled]
[Enabled]
[Enabled]
[Enabled]
[CDROM]
[Floppy]
[HDD-0]
[Enabled]
[Disabled]
[On]
[Fast]
[Enabled]
[Disabled]
[Setup]
[Non-OS2]

Item Help

On some **Dell Systems** you can enter bios by pressing F2

```
F2 = Setup
F12 = Boot Menu
```

Now choose Boot Sequence and then arrance 1 to CD-Rom by pressing - + and press space to enable it
Press ESC and choose save settings and exit

```
Dell - Dimension 8100
Intel Pentium 4 Processor: 1.30 Ghz
LEVEL 2 Cache: 256 KB Integrated

System Time ..................
System Date ..................

Primary Drive 0 ..............
Primary Drive 1 ..............
Secondary Drive 0 ............
Secondary Drive 1 ............

Boot Sequence ................
* 1. IDE CD-ROM Device
* 2. Hard-Disk Drive C:

SPACE to enable/disable | +,- to move down/up

System Memory ................
AGP Aperture .................
CPU Information ..............

Up/Down to Select | SPACE +,- to Change | ESC to Exit
```

On some **Dell Systems** you can enter bios by pressing F2

```
Boot Device Menu
________________

  1. Normal
  2. Diskette Drive
  3. Hard-Disk Drive C:
  4. IDE CD-ROM Device

Enter a choice: 1
```

Sometimes you can press F12 to temporary boot from cd on some **Dell Systems**

```
PhoenixBIOS 4.0 Release 6.0
Copyright 1985-1999 Phoenix Technologies Ltd.
All Rights Reserved
Copyright 1996-1999 Intel Corporation.
4S4EB2X0.05A.0009.P08

Micron Electronics, Inc.

Intel(R) Pentium(R) III processor 450 Mhz
640K System RAM Passed
255M Extended RAM Passed
512K Cache SRAM Passed

Press F2 to Enter Setup
```

Press F2 to enter bios setup

```
ROM PCI/ISO BIOS (P2B-DS)
CMOS SETUP UTILITY, AWARD SOFTWARE, INC.
STANDARD CMOS SETUP

BIOS FEATURES SETUP

CHIPSET FEATURES SETUP

POWER MANAGEMENT SETUP

PNP AND PCI SETUP

LOAD BIOS DEFAULTS

LOAD SETUP DEFAULTS

SUPERVISOR PASSWORD

USER PASSWORD

IDE HDD AUTO DETECTION

SAVE & EXIT SETUP
```

and set Boot Sequence to A,CDROM,C and Press Esc and then F10 to save it.

ROM PCI/ISO BIOS (P2B-DS)
CMOS SETUP UTILITY, AWARD SOFTWARE, INC.

CPU Internal Core **Speed**
Boot **Virus Detection**
Processor Serial Number
CPU Level 1 Cache
CPU Level 2 Cache
CPU Level 2 Cache ECC Check
BIOS **Update**
Quick Power On Self Test
HDD Sequence SCSI/IDE First
Boot Sequence
Boot Up Floppy Seek
Floppy Disk Access Control
IDE HDD Block Mode Sectors
HDD S.M.A.R.T. capability
PS/2 Mouse Function Control
OS/2 Onboard Memory > 64M
MPS 1.4 Support
650Mhz
Enabled
Disabled
Enabled
Enabled
Disabled
Enabled
Enabled
IDE
A,CDROM,C
Disabled]
R/W
HDD MAX

Some Computer has Option to temporary boot from Cd/Hdd/Floppy/Usb Device, Just keep tapping the F8 button to get **Boot Menu** and Now choose your manufacture of CDRom.

مهم جدا أن تجعل الجهاز يقلع من DVD وذلك حتى يتمكن النظام من التثبيت

تضغط على أي زر بشكل متقطع حتى يتم الدخول إلى شاشة الإعداد الزرقاء

```
Setup is inspecting your computer's hardware configuration...
```

هذه هي شاشة الإعداد الرئيسية تنتظره حتى تظهر لديك الخيارات ، أما الآن فهو يحمل الملفات الرئيسية بنفسه ، التي سيستخدمها أثناء الإعداد ..



هذه الشاشة تخبرك بأنه لتثبيت نظام جديد اضغط Enter

أما لإصلاح النظام الجديد اضغط حرف R من لوحة المفاتيح ..

وطبعا سنضغط Enter لتثبيت نظام جديد ، وتذكر الجملة التالية ستتكرر كثيرا

الوقـــاية خير من العـــلاج ..

```
Windows XP Professional Setup

  Welcome to Setup.

  This portion of the Setup program prepares Microsoft(R)
  Windows(R) XP to run on your computer.

      •  To set up Windows XP now, press ENTER.

      •  To repair a Windows XP installation using
         Recovery Console, press R.

      •  To quit Setup without installing Windows XP, press F3.

  ENTER=Continue   R=Repair   F3=Quit
```

تضغط زر F8 من لوحة المفاتيح سواء وافقت أم لم توافق على اتفاقية الاستخدام ☺



تقوم باختيار القرص الذي تريد التثبيت عليه ، ثم الضغط Enter



هنا تختار نوع تهيئة القسم الذي تريد التثبيت عليه ، يفضل جدا أن يكون NTFS

وذلك لأنه أفضل كثيرا وأسرع من نظام FAT ولن نشغل بالكم بالفروقات البرمجية بين النظامين إلا اختيار السطر الأول هو الأفضل :)

Windows XP Professional Setup

The partition you selected is not formatted. Setup will now format the partition.

Use the UP and DOWN ARROW keys to select the file system you want, and then press ENTER.

If you want to select a different partition for Windows XP, press ESC.

Format the partition using the NTFS file system (Quick)
Format the partition using the FAT file system (Quick)
Format the partition using the NTFS file system
Format the partition using the FAT file system

ENTER=Continue ESC=Cancel

سيبدأ بنسخ الملفات اللازمة ، ثم يعيد التشغيل تلقائيا

Windows XP Professional Setup

Please wait while Setup formats the partition
C: Partition1 [New (Raw)] 4087 MB (4086 MB free)
on 4095 MB Disk 0 at Id 0 on bus 0 on atapi [MBR].

Setup is formatting... 20%

الشاشة الجديدة التي توضح بداية العمل بويندوز اكس بي :)



هذه تظهر لكي تضع الإعدادات الخاصة بك ، وغالبا ما تطلب منك إدخال مفتاح المنتج Product Key وتجده في نفس النسخة وهو مكون من ٢٥ حرف ننصح بعدم محاولة تجريب تثبيت أي نظام تشغيل إلا بعد التجريب على الأنظمة الوهمية حتى تتمكن من تخطي أي مشكلة أو عقبة .



بعد تثبيت الويندوز تظهر أمامك شاشة تخبرك بكتابة اسم مستخدم الكومبيوتر ، وتستطيع إنشاء أكثر من مستخدم ، حتى يتم الفصل بينهم في إعدادات البرامج والمستندات ، ورموز سطح المكتب وما إلى ذلك .

Microsoft Windows xp

Who will use this computer?

Type the name of each person who will use this computer. Windows will create a separate user account for each person so you can personalize the way you want Windows to organize and display information, protect your files and computer settings, and customize the desktop.

Your name: Daniel Petri
2nd User:
3rd User:
4th User:
5th User:

These names will appear on the Welcome screen in alphabetical order. When you start Windows, simply click your name on the Welcome screen to begin. If you want to set passwords and limit permissions for each user, or add more user accounts after you finish setting up Windows, just click **Control Panel** on the **Start** menu, and then click **User Accounts**.

For help, click here or press F1.

Back Next

وبهذا يكون انتهى تثبيت نظام ويندوز XP بالكامل ، العملية سهلة وننصحك بتجريبها بعد درس الأنظمة الوهمية .

موفقين بإذن المولى ..

الدرس الثالث :: تثبيت نظام ويندوز سيفين

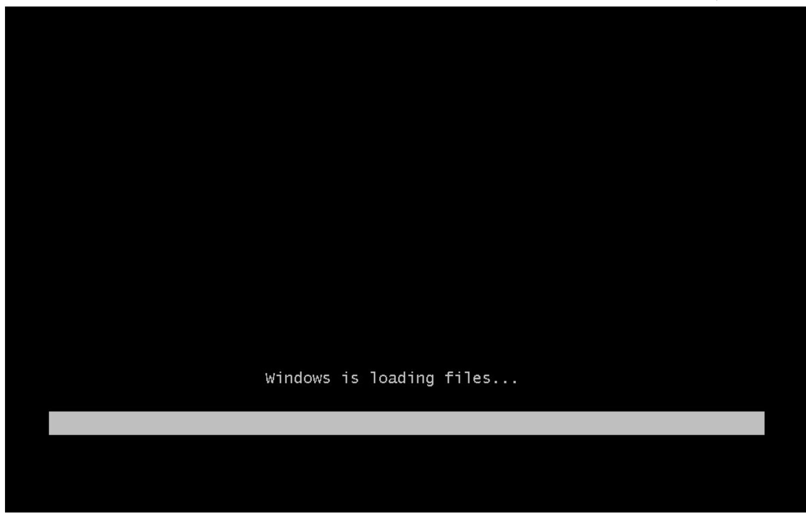
Windows Seven 7

أحدث ويندوز حتى الآن من شركة مايكروسوفت ، ولكنه غير مرغوب من كثير من المستخدمين خصوصا العاديين وذلك لأنه يستهلك الذاكرة وبطيء على الأجهزة القديمة ، بالإضافة إلى أن كثير من البرمجيات لا تعمل عليه .

ليس هذا فحسب فيتهمه الكثيرين انه جاء للمرفهين والذين يستطيعون استبدال أجهزتهم بشكل مستمر ، أو تطوير مواصفاتها .

وتوعدت كثير من الشركات أنها تدعم إنتاج الويندوز القادم والذي من المفترض بعد عدة تصريحات أن لا يعمل على معظم الأجهزة المتواجدة لدى المستخدمين ، في إشارة لضرورة استنفاع شركات الحاسب من بيع وتطوير الحاسبات .

يتشابه تثبيت ويندوز سيفين مع ويندوز اكس بي في ضرورة أن يتم الإقلاع من السواقة التي تحتوي نظام التشغيل المراد تثبيته حتى يتم الدخول إلى شاشة الإعداد فلنتابع معاً ، بعد وضع الاسطوانة تظهر هذه الشاشة وهي الشاشة التي تحضر للدخول لشاشة الإعداد الرئيسية .



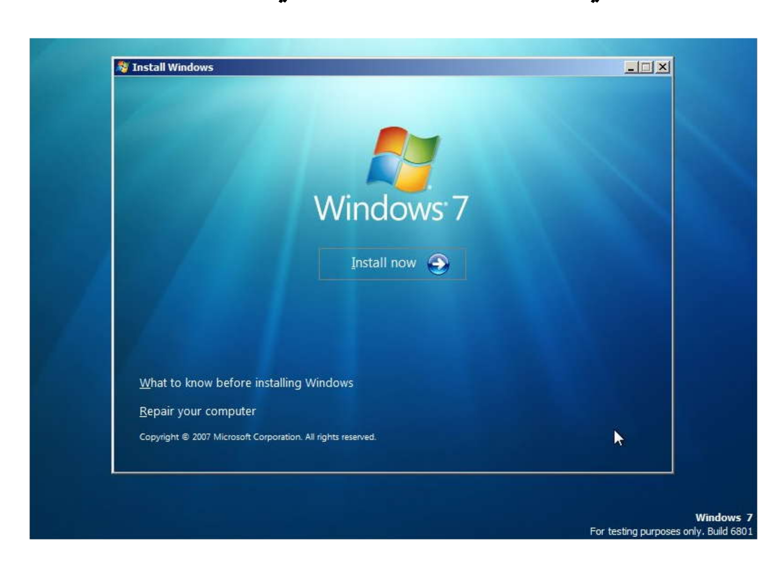
بعدها سيظهر معالج الإعداد بالشكل التالي ::



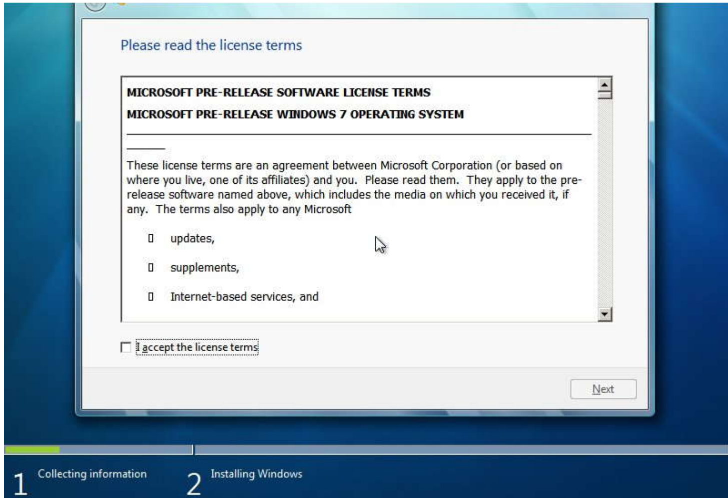
هنا يتم إخبارك باللغة الافتراضية المطلوبة للتثبيت ،



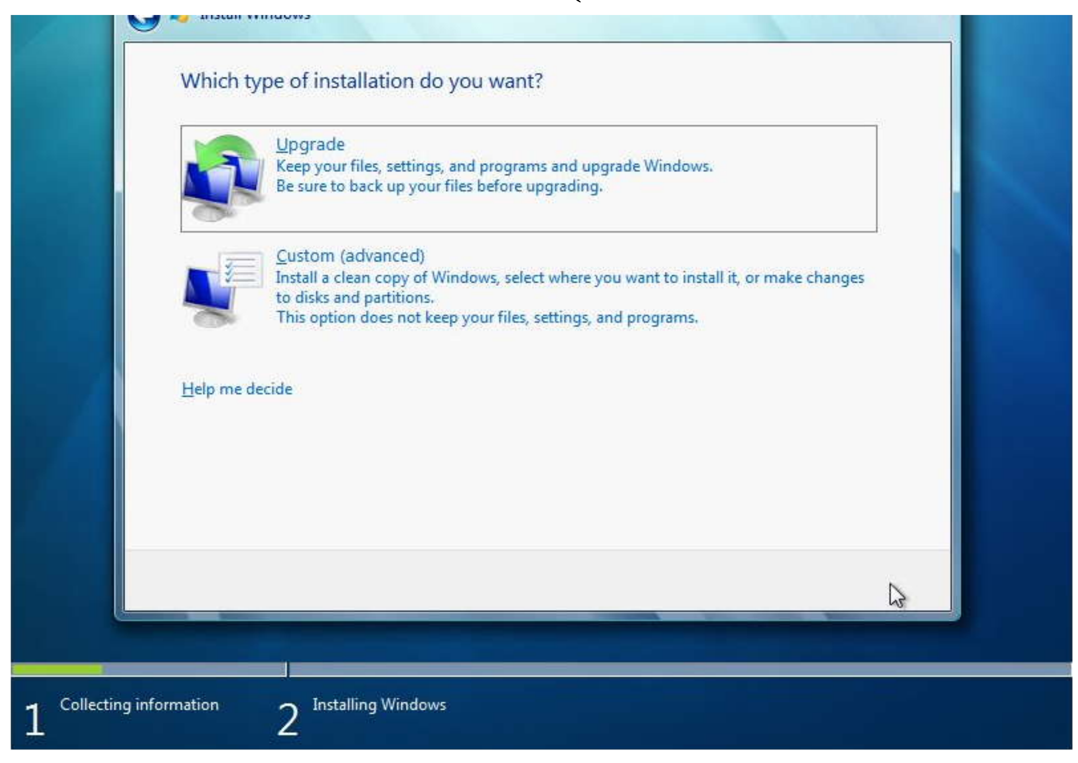
تضغط Install Now أو في نسخة الويندوز العربي التثبيت الآن



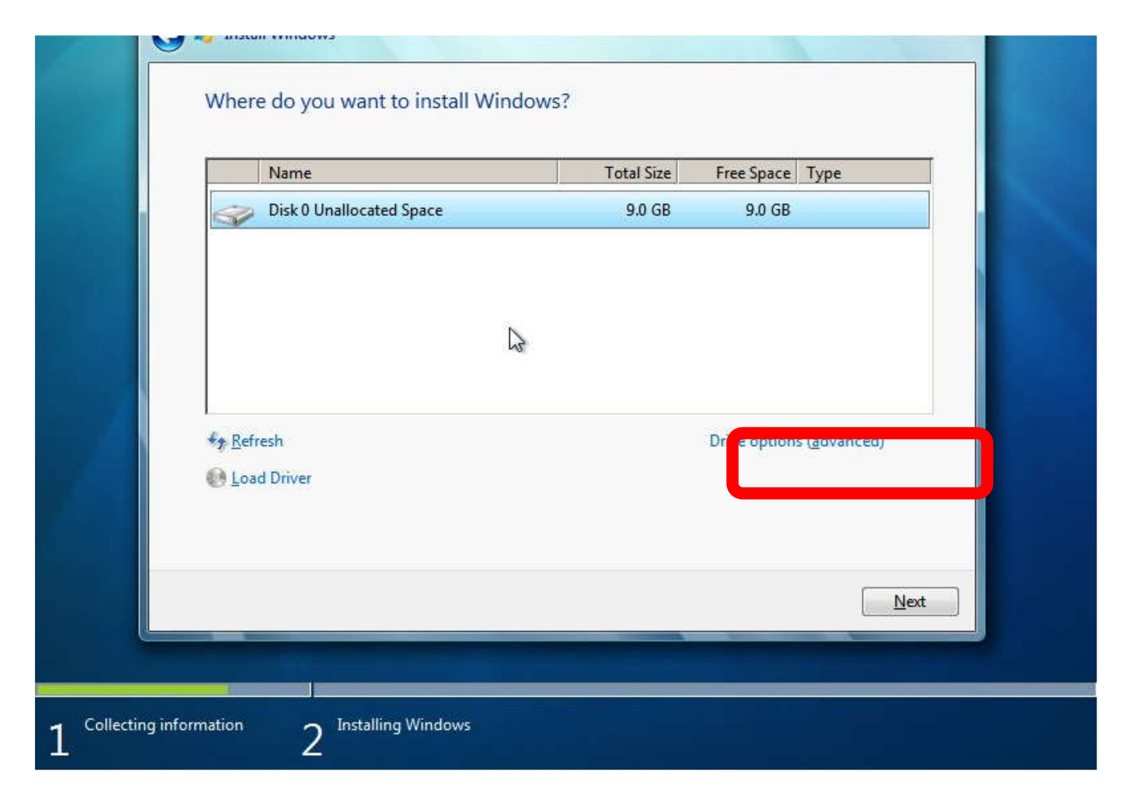
تظهر اتفاقية المستخدم وطبعا تضغط زر I accept أو أنا أوافق في النسخة العربية



هنا يتم إخبارك بالتحديث أو بالتثبيت الاختياري ، ننصح أن يتعامل المستخدم مع الأنظمة الوهمية ويرى الفروق بنفسه :)

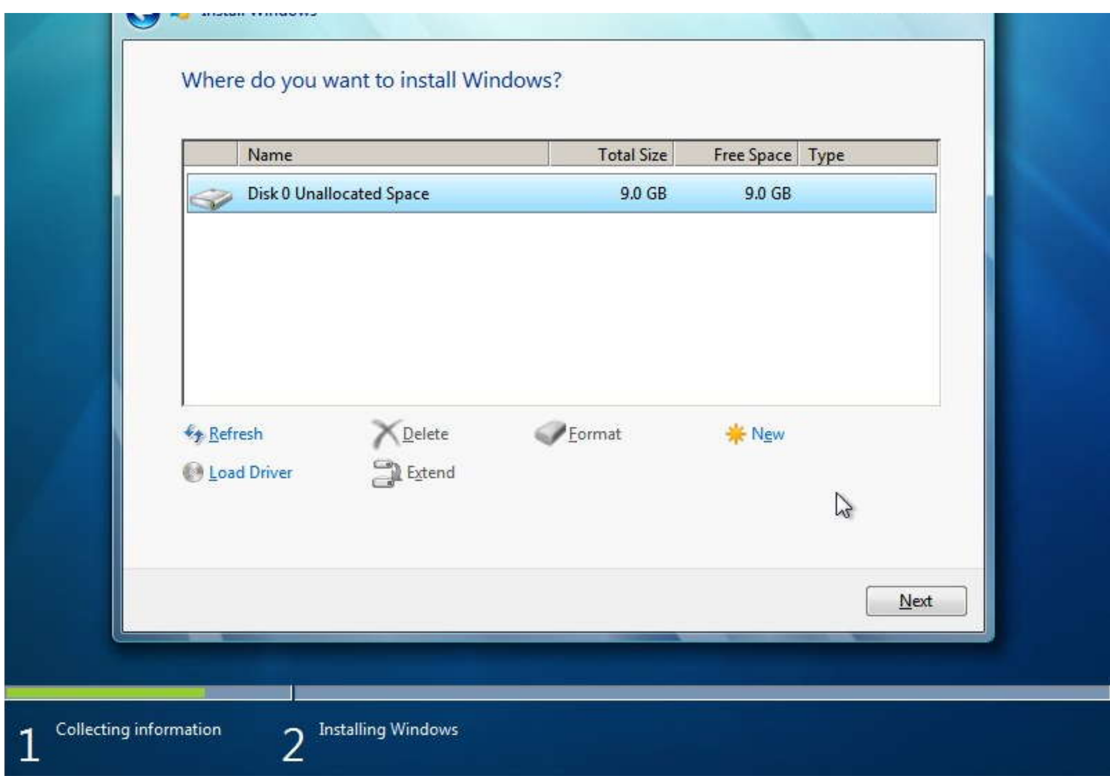


هذه الشاشة ستظهر إذا كان الهارد الخاص بك غير مقسم ولم يكون عليه أي نظام تثبيت في السابق ، ستضغط على زر Drive options أو في النسخة العربية خيارات الأقراص

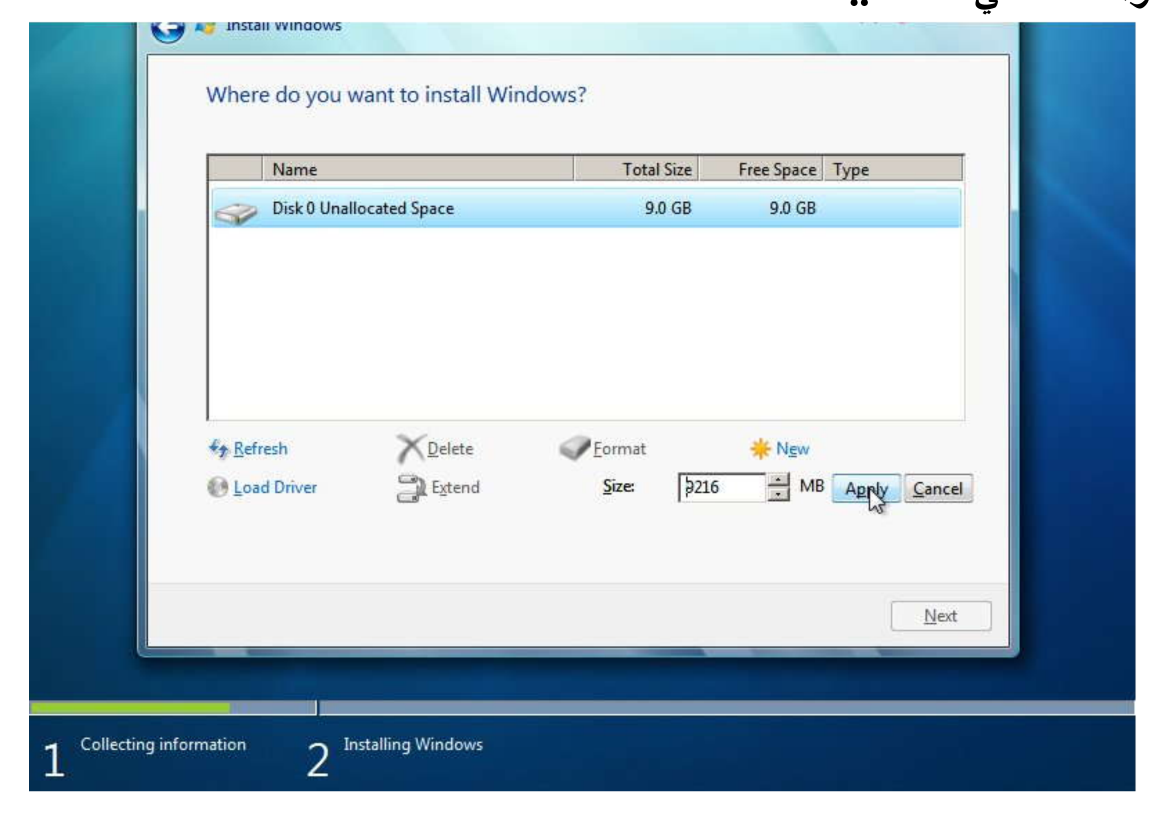


هذه هي الخيارات تضغط على زر New لإنشاء قسم جديد بالمساحة التي تريدها ،

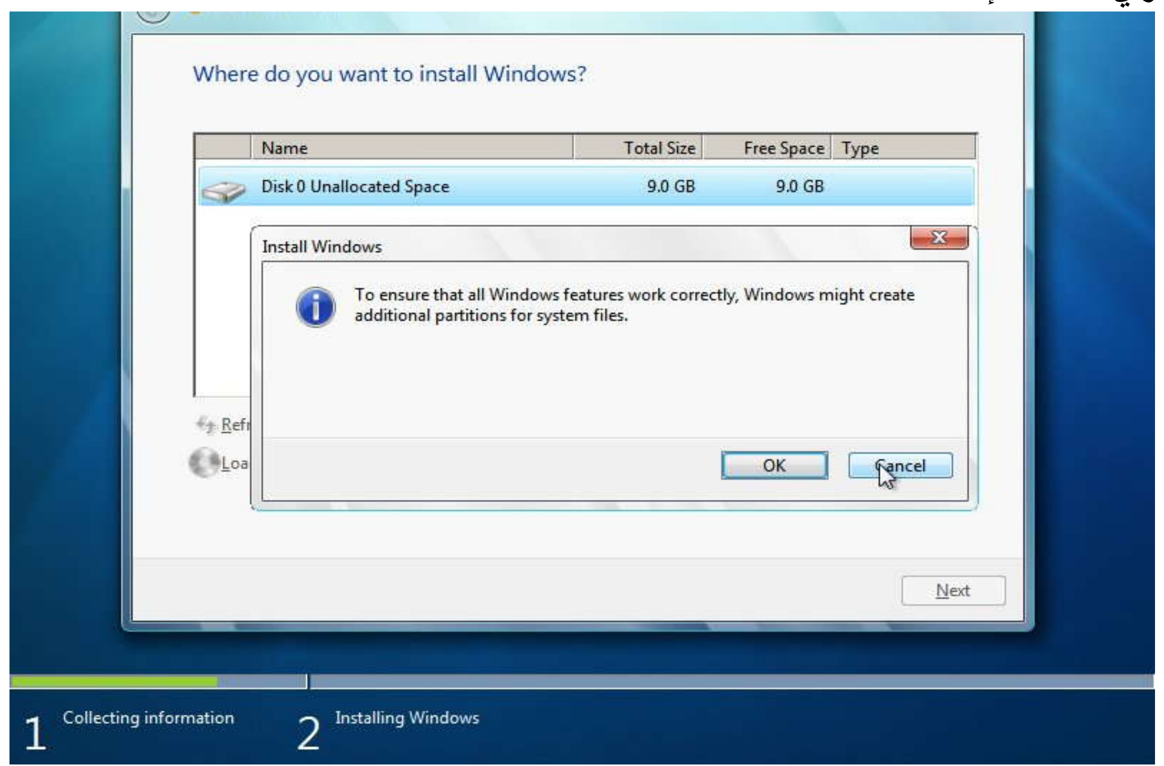
ملاحظة ستجد نفس الشرح فيديو لكثير من الدروس :)



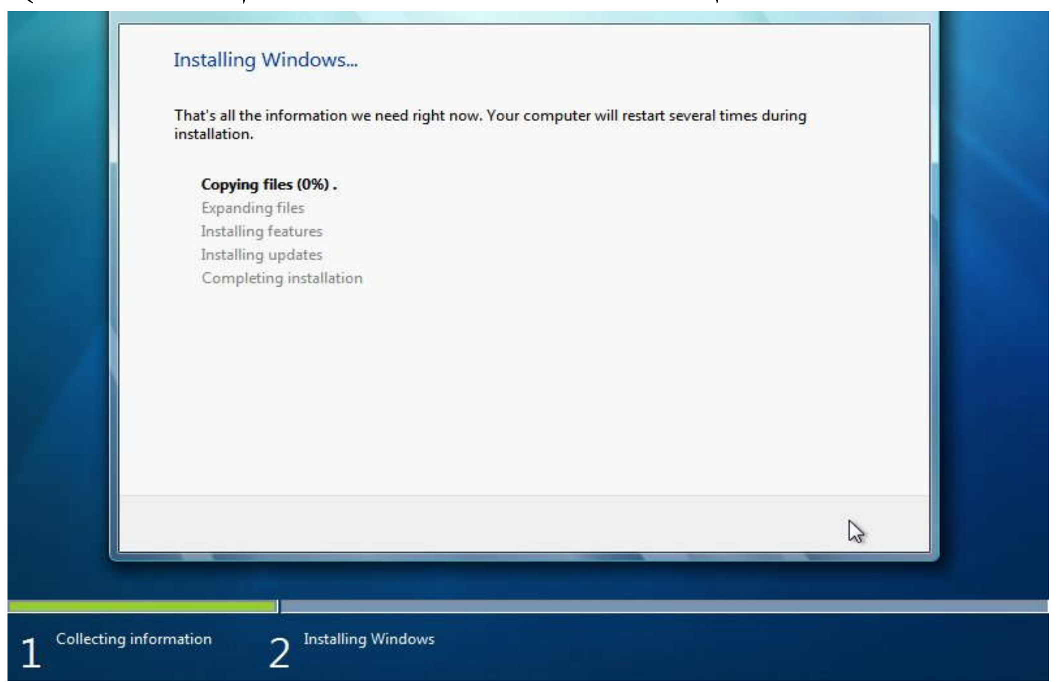
سيتم ظهور الحجم الذي تريده للقسم الأول ، إذا تركته كما هو سيتم إنشاء قرص واحد فقط في نظامك ..



عند ظهور هذه الرسالة أضغط Cancel لكي لا يتم إنشاء قرص آخر لنظام صغير يحوي ملفات الإعداد ..



هنا يبدأ الإعداد بتثبيت النظام وسيعيد التشغيل ليظهر لديك النظام مثبت وكامل :)



تستطيع الحصول على مساعدة ضخمة من خلال البحث أكثر عن هذه العمليات ، وتستطيع أيضا رؤية الشرح فيديو صوت وصورة إذا ما دخلت على المدونة الخاصة ، وستجده في الغالب بنفس عنوان الدرس .

الدرس الرابع :: الأنظمة الوهمية

شرح برنامج Microsoft Virtual Machine

يعتبر من أهم البرامج الآن للهواة والمتخصصين ، والكثيـــرين من الأشخاص الذين يعتمدونه في الحماية وفي التصفح الآمن والاستخدام الشخصي الفعال .

بالنسبة لي أنصح الجميع بأن يثبت هذا البرنامج أو غيره من برامج الأنظمة الوهمية ، ويتعلم كيفية إنشاء نظام وهمي لأن أغلب الهاكرز المتواجدين في الساحة الآن لا يستطيعون التنقل إذا ما تم اختراق النظام الوهمي للنظام الحقيقي .

سيتم تسمية النظام الأساسي بالحقيقي ، أما النظام التابع للبرنامج الوهمي ، سيسمى بالنظام الوهمي ، وذلك لأنه يعتمد على النظام الحقيقي ، ويستخدم لكثير من الاستخدامات أهمها الأمن والفحص والتدقيق ، فلو تم إلحاق الضرر أو تشغيل فيروس معين لن يتم تجاوز النظام الوهمي على الإطلاق ، وسيتجمد الفيروس داخله ، وبكل سهولة نستطيع حذف النظام الوهمي كأي ملف موجود لدينا ، وإنشاء نظام جديد في وقت بسيط ..

حينها سنؤمن معلوماتنا الشخصية وبرامجنا المهمة ، وأعمالنـــا والكثير .

وستلاحظ أن برامج الأنظمة الوهمية هي أهم البرامج لخبراء الهاكرز وأطفالهم على حد سواء ، إلا أننا سنستخدمه في إنشاء عدة نظم مختلفة ، واحد سيكون للفحص والتدقيق ، وآخر لتصفح الانترنت أو عمل المحادثات وما إلى ذلك .

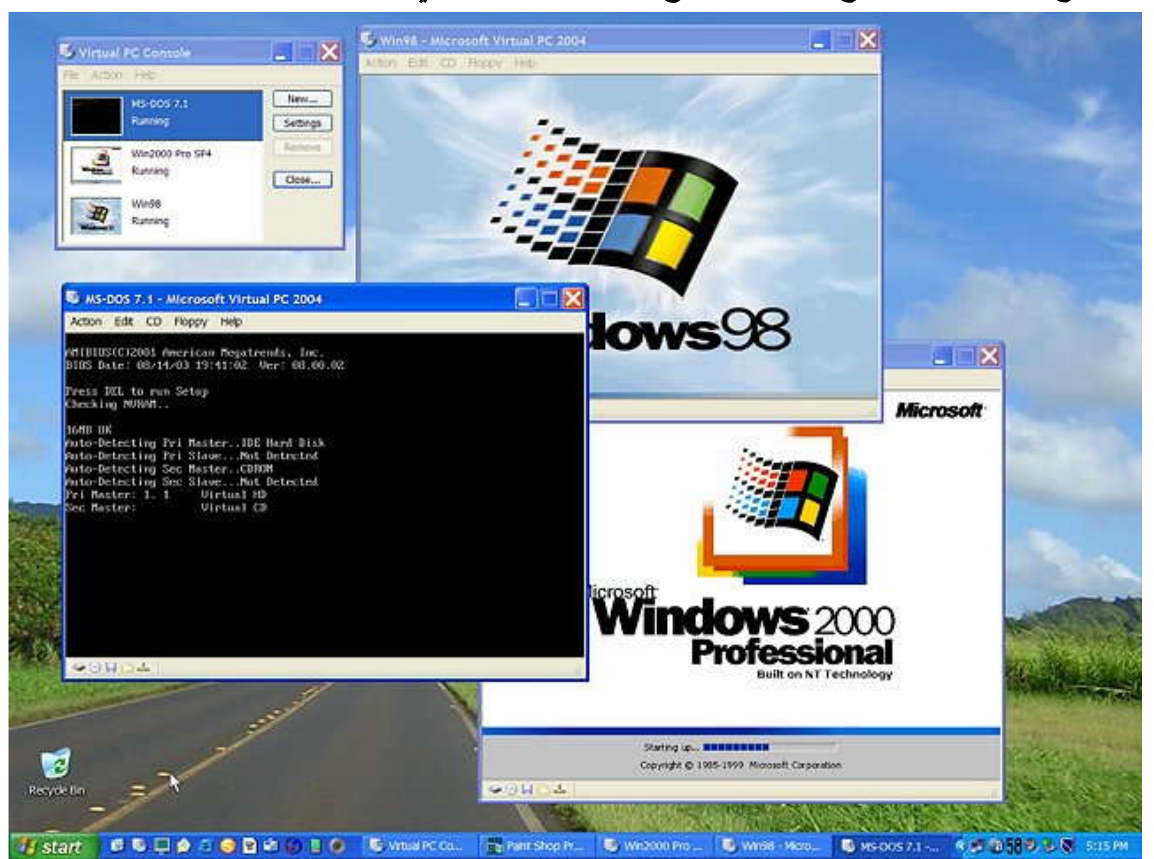
ويستطيع المستخدم منكم إنشاء المزيد من الاستخدامات والأهداف بنفسه بعد الخطوات الأولى التي سنخطها معاً بإذن الله .

راجياً من الله عز وجل أن ينعم عليا وعليكم وعلى جميع بني البشر بأرض تخلو نم الشر ، وحصن لا يمكن تجاوزه ، اللهم أنعم علينـــا بالستر ، ويسر أمورنـــا ، وانصرنـــا على القوم الكافرين والمنافقين ..

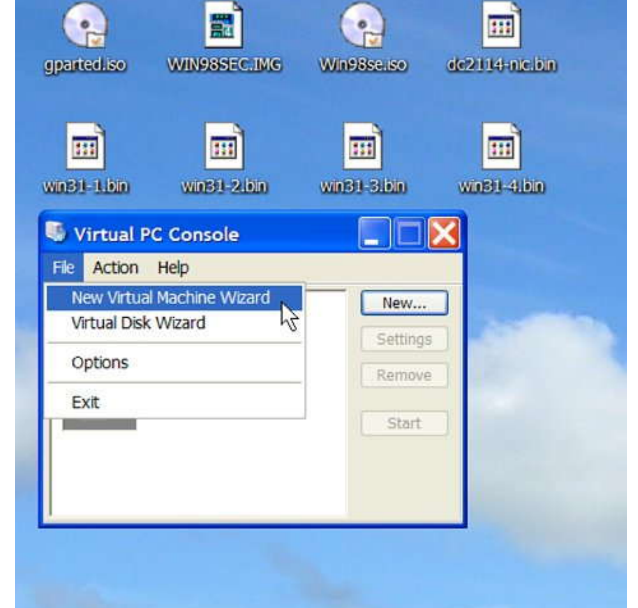
نبـدأ على بركة الله أولى الشروحات الفعلية التي يجب تطبيقها كـ مستخدم عادي للوصول للحماية المتكاملة ، صدقني ستصبح تتحدى الهاكرز بإظهار مهاراتهم في اختراق جهازك لو كانوا يحملون تلك المهارات أصـــلا ، ولن يستطيعوا..

إلا لو كانوا الحكومة طبعاً ، بيخترقوا جهازك وبيتك أكيد !!

تستطيع تحميل البرنامج من موضوع خاص بالدرس في المدونة .

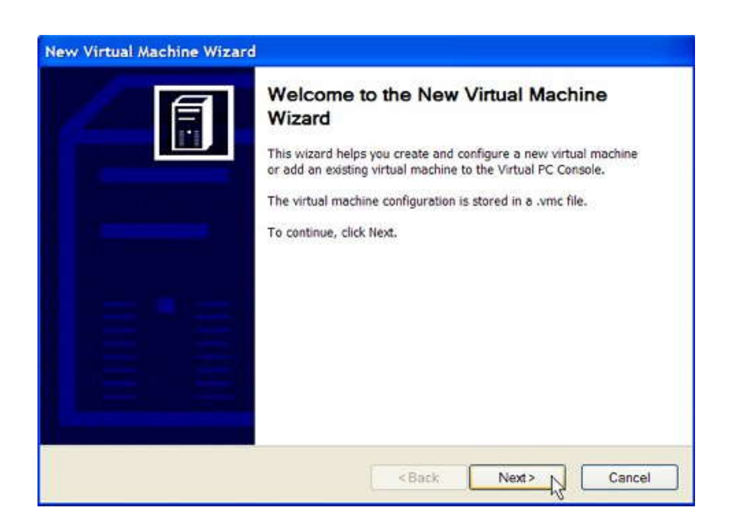


هذا ما ستحققه بإذن الله من خلال هذا الشرح ، العديد من الأنظمة تعمل من خلال نظامك الأصلي ، تستطيع تثبيت عشرات الأنظمة والأنواع ، وتجربة مئات النسخ ، فتابع معنا وستجد الموضوع في غاية السلاسة والبساطة ، والمتعة أيضاً ..

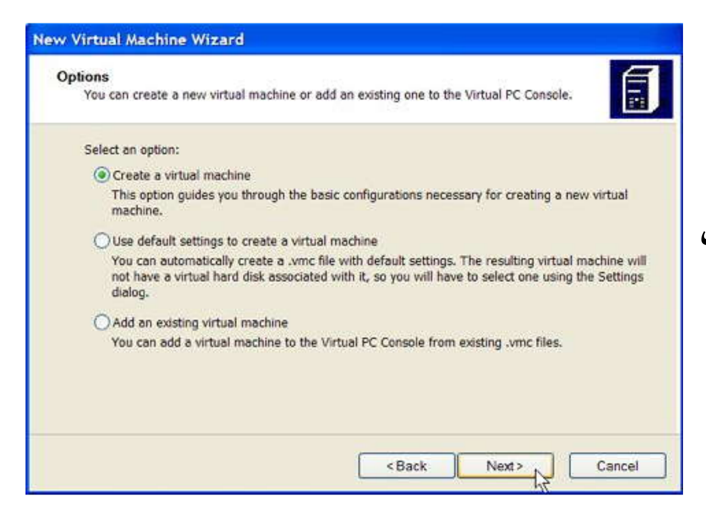


خطوات إنشاء نظام وهمي ::

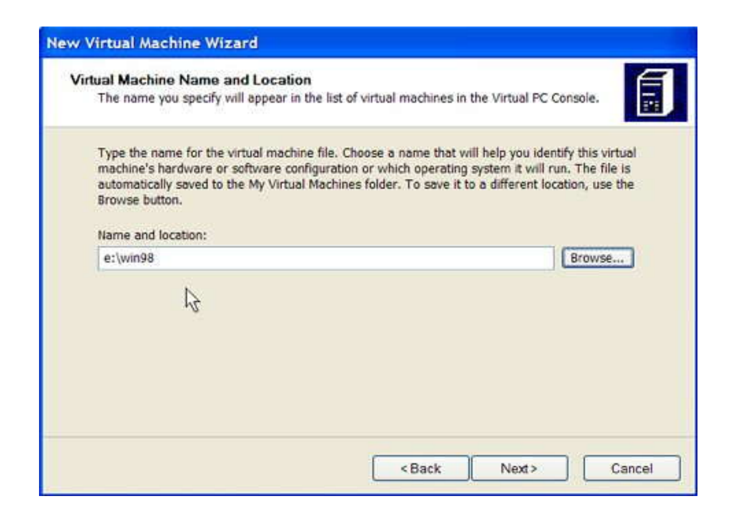
١ – بعد تثبيت البرنامج كأي برنامج آخر ، نضغط **File** ثم **New Virtual Wizard** لإظهار الخيارات المتقدمة لإنشاء نظام وهمي ..



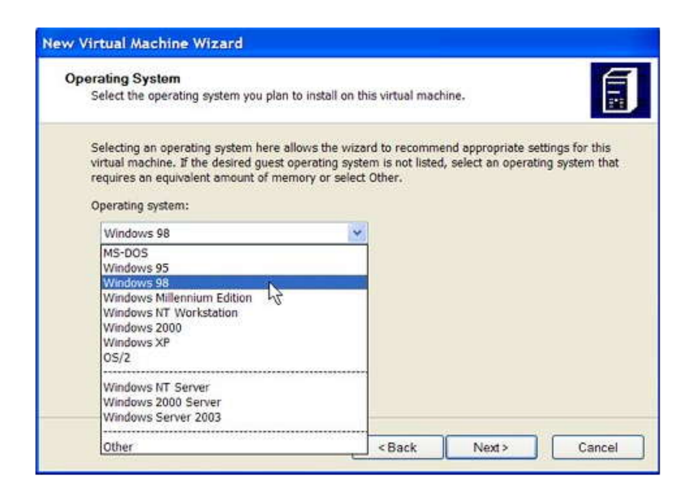
٢ – تضغط Next حتى تنتقل للخطوة القادمة من رحلة إنشاء نظام وهمي داخل نظامك الحقيقي



٣ – تختار الخيار الأول ، وهو خاص بإنشاء هارد درسك جديد ، بمساحة أنت تحددها ، وسنرى معاً كيفية فعل ذلك في الخطوات القادمة ..

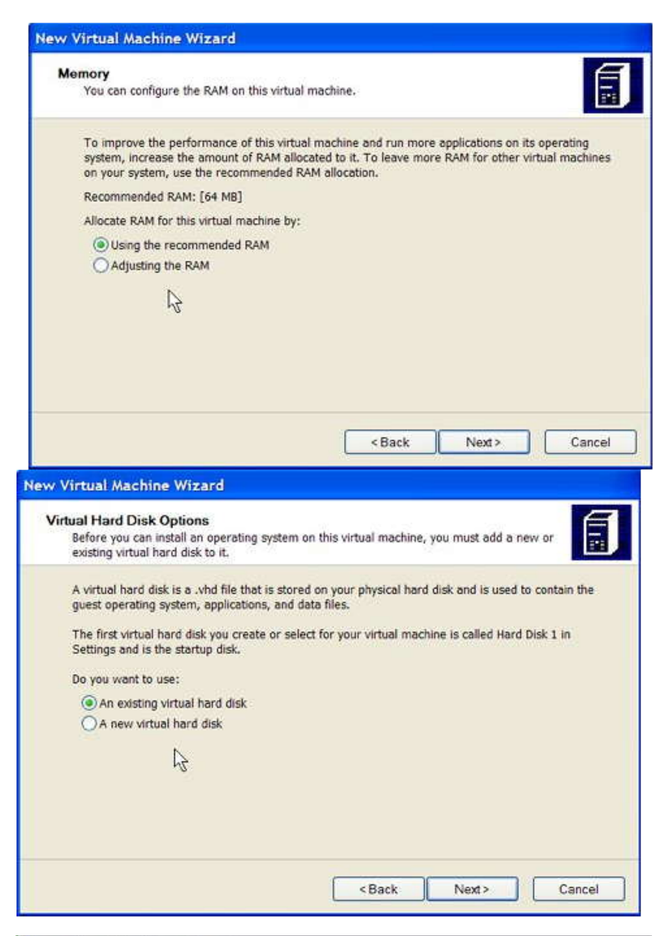


٤ – نختار مكان حفظ النظام الوهمي ويفضل اختيار قرص يحتوي على مساحة فارغة كبيرة ، ونختار اسم للنظام الذي سيتم إنشاؤه .



٥ ـ هذه الشاشة ستساعدك في إظهار الأنسب للنظام ، ولكن تستطيع عدم التقيد بها واختيار الخيار الأخير **Others** أو اختيار اسم النظام .

فأنت حر في بعض الأحيان :) ..

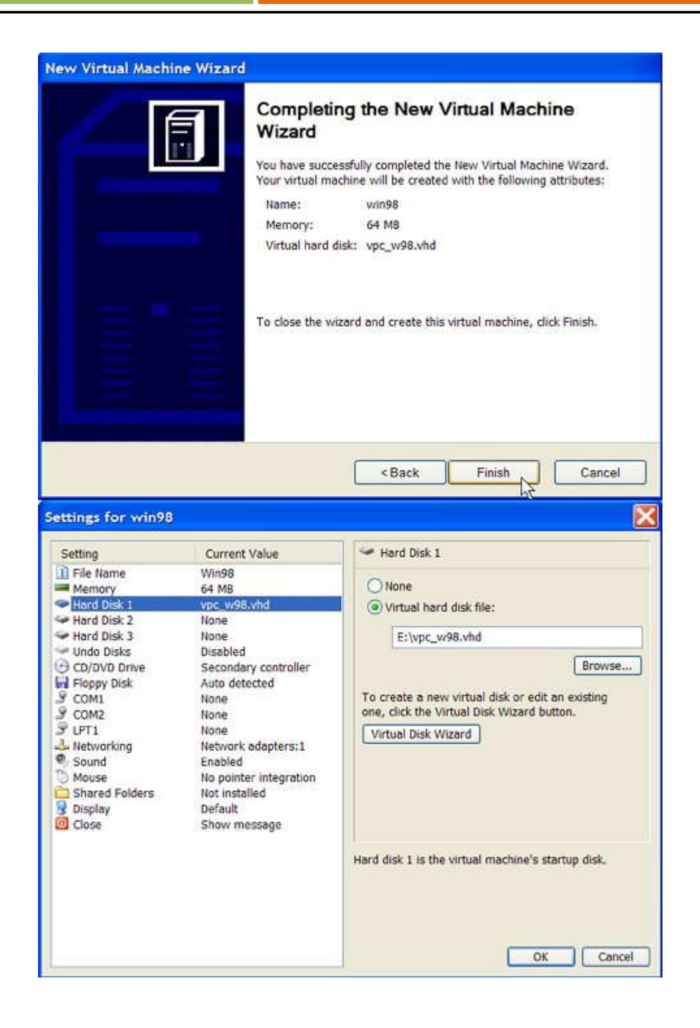


٦ ـ هنا يخبرك بأن الذاكرة الافتراضية المناسبة للنظام ١٢٨ ميقا بايت وتستطيع تعديلها بالضغط على الخيار **Adjusting the RAM** وطبعا لن تتم زيادتها عن الذاكرة الحقيقية

٧ ـ هنا يخبرك الخيار الأول اختيار هارد درسك قديم ، بمعنى لو كان بالفعل نظام قديم لديك في قرص آخر ، أما الخيار الثاني فهو إنشاء هارد سك وهمي جديد وهو ما سنختاره في البداية .



٨ ـ تختار حجم الهاردسك المراد إنشاؤه للنظام الوهمي ، وطبعا لن تستطيع اختيار أكبر من المساحة الفارغة في القرص الأساس



٩ – ثم تضغط **Finish** للانتهاء .

١٠ – إذا أردت تعديل أي إعدادات

بعد إنشاء النظام الوهمي الجديد

تضغط على زر **Settings**



١١ – تضغط زر **Start**

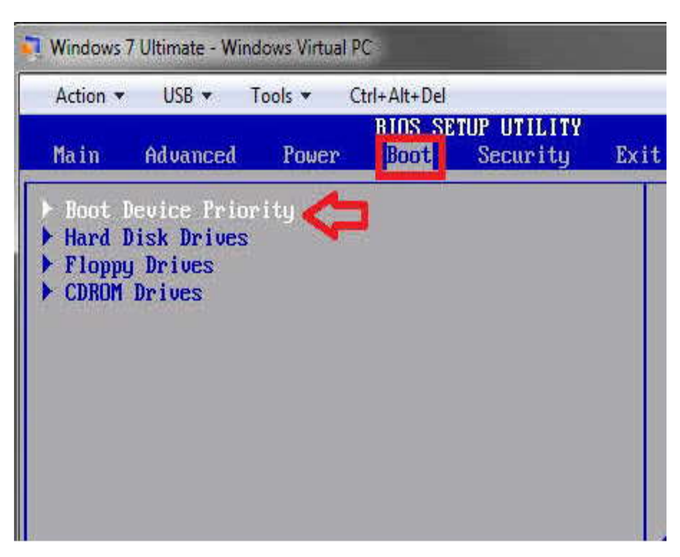
أو تنقر مرتين على الآلة التي تم إنشاؤها

لتبدأ بالعمل .

بعدها حاول الدخول إلى Bios Setup لتغير إعدادات الإقلاع وتختار أول جهاز تبدأ الآلة الوهمية بقراءته هو DVD وذلك حتى تختار الاسطوانة التي تحتوي النظام ، هناك درس مهم عن برنامج يستخدم في تحويل الاسطوانات الى ملف دائم على الجهاز الشخصي حتى يريحنا من تكرار وضع الاسطوانات ، أو حفظ الاسطوانات لمحاولة نسخها لاحقا لو حدث لها عطب ما ، واسمه Ultra ISO

نكمل الشرح ..

١٢ ــ نضغط فور تشغيل الآلة بشكل متقطع زر F2 و Del من لوحة المفاتيح وذلك حتى ندخل إلى Bios Setup فلو لم تنجح العملية نكرر إعادة تشغيل الجهاز حتى ننجح وتظهر لنا هذه الشاشة

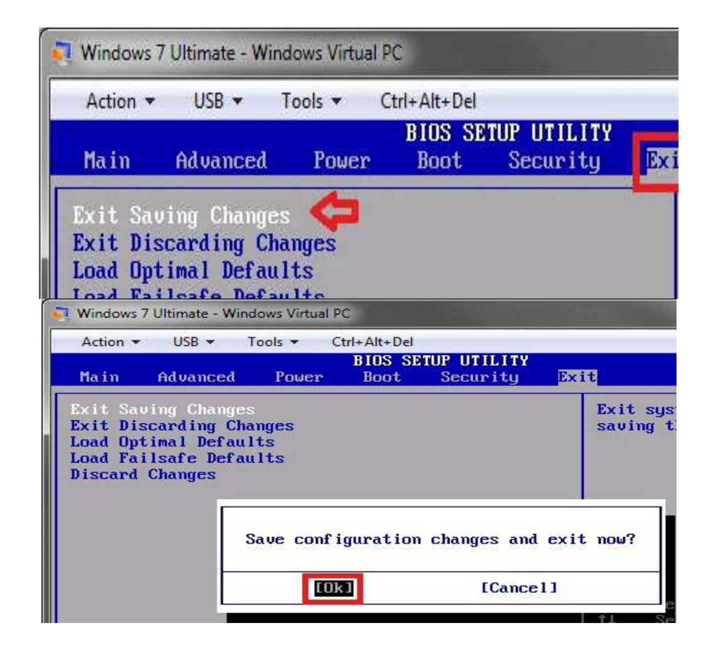


١٣ ــ ، نذهب إلى قائمة Boot كما نرى من خلال زري الزائد والناقص نجعل أول جهاز هو CDROM لكي نثبت نظاماً جديداً .



١٤ ــ نذهب بعدها إلى قائمة Exit ونحفظ الإعدادات الجديدة ، أو نختصر الأمر بالضغط على زر F10 من لوحة المفاتيح .

١٥ ــ عند ظهور هذه الشاشة نضغط Enter فتعيد الآلة تشغيل نفسها ويبدأ تثبيت النظام الجديد (:



لمعلومات أكثر تستطيع مشاهدة الفيديو المفصل لعملية الشرح وتثبيت النظام الوهمي بالكامل ، وهو شرح بالصوت والصورة تحت اسم نفس الدرس ، أما من حمل الدورة كاملة فسيجده ق١ – د٥ وذلك لأني حذفت الدرس الخاص بويندوز فيستا لعدم وجود مستخدمين يهتمون بهذا الإصدار ، بل واندثار أكثر المعجبين به الآن بين إصداري ويندوز اكس بي وسيفين .

تستطيع تشغيل ويندوز اكس بي كـ حقيقي ، وويندوز سيفين كـ وهمي .

والعكـــس ..

تستطيع أيضا تجربة عشرات الأنظمة الأخرى كـ الماك اللينكس وغيرهم .

تستطيع تشغيل أكثر من نظام وهمي في وقت واحد ،

تستطيع التنقل بكل سهولة من بين نظام وآخر ،

تستطيع أيضاً فصل الانترنت عن أي نظام مع استمراره في نظام آخر .

تستطيع نقل الملفات بين الويندوز الحقيقي والوهمي بأكثر من طريقه .

تستطيع تجربة آلاف التجارب على الجهاز الوهمي قبل تجريبها على الحقيقي ،

فاكتساب الخبرة في البداية هو الطريق الأمثل للتعلم .

ومن ثم استثمر طاقتك ، واستعرض عضلات عقلك .

وعلم مثلما تم تعليمـــك ..

ابتكر دائما ، ولا تمل من الأخطاء ، كرر فمرة بعد أخرى ستتمكن من تخطي ما كنت تعتقده في الماضي من المستحيـلات .

و من عاش على الأمل لا يعرف المستحيل .

بوجود الرب الرحمن لا تيأس يا إنســـان ..

وفقكم الله

ادعوا لنـــا جميعاً فقد نكون بحاجة لأبسط دعاء ،

الدرس الخامس :: التعريفات

الجزء الأول اسطوانة التعريفات الشاملة

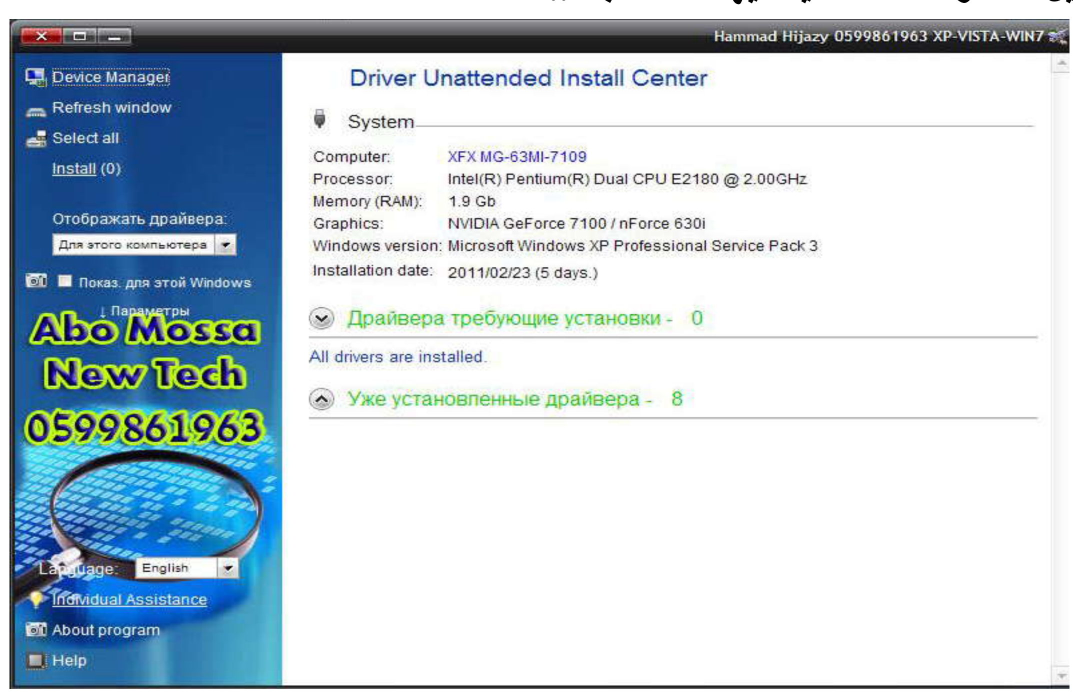
اسطوانة تم انتشارها في الانترنت بواسطة أشخاص لهم الفضل من بعد الله عز وجل ، في حل مشكلة من أهم المشاكل التي كانت تواجه الأفراد والشركات ، وخصوصا محلات الصيانة ..

لذا ركز بعد تعلمك أن هذا العلم البسيط داخل هذا الكتاب قد يكون بداية لدخولك مجال صيانة الحاسب الآلي عبر فتح محل متخصص في الحاسب ، لكن أنا شريك معكم لا تنســوا :)

نتمنى لكم التوفيق ، أول شيء .

فهذه البرمجية الرائعة تم تطويرها بشكل مستمر ، حتى وصلت الآن إلى شكل رائع ومميز ومساحة جيدة ، تقريبا ٣٠٠ ميقا بايت تحوي أكثر من ١٠٠ ألف تعريف لقطع الهاردوير ، ويتم تحديثها بشكل مستمر تبعا للتطورات التي تحدث في مجال إنتاج قطع الهاردوير ..

أما الشرح الكامل فستجده فيديو ، لأن كل اسطوانة تختلف عن الأخرى ، ولكنها تتشابه في بعض أوامر الواجهة الرئيسية وهي سهلة جداً ، ولا تحتاج دروس مطولة ، وشروحات معقدة كما يحدث من البعض داخل الانترنت ، بل وتستطيع تعديل المعلومات الداخلية فيها ، لتناسبك ..

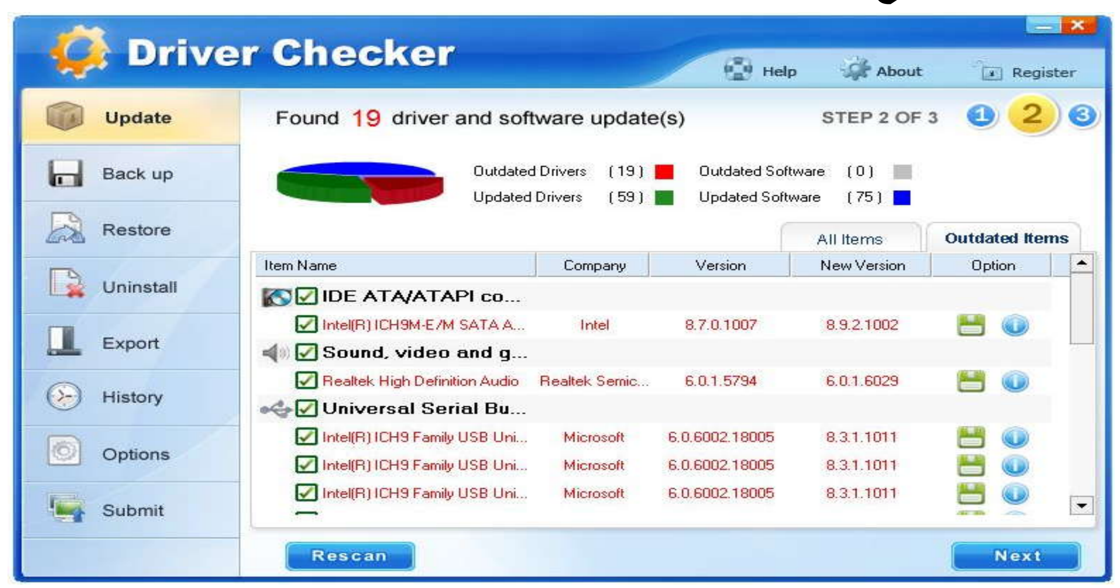


الجزء الثاني :: برامج التعريفات

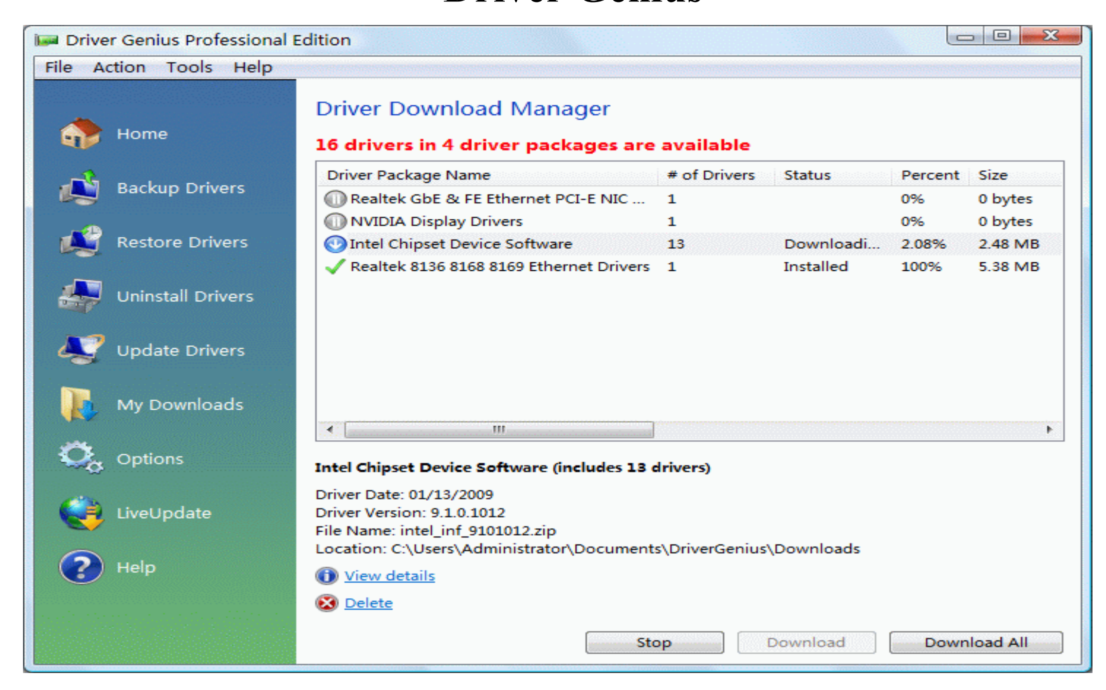
هناك درسي فيديو للجزء الأول والثاني يشرحا بالضبط هذه البرمجيات بشكل سلس وهما الجزأين ق١ د٥ ج١ ، ق١ د٥ ج٢

بالنسبة لبرامج التعريفات فهي سهلة جدا ، وتتشابه في أنها تحتوي على قاعدة بيانات ضخمة ، تبحث في جهازك عن القطع الغير مثبتة وتقارنها بقاعدة البيانات ثم تجلب لك التعريفات من خلال الانترنت .

وأمثلة عليها برنامج Driver Checker Database



Driver Genius



الدرس السادس : فنون التصفح الآمن

Mozilla FireFox

البرنامج الرائع المجاني ، الذي يتم دعمه بشركات عملاقة ، وبخبراء في مجال الحاسب الآلي ، ويعتبر الآن أضخم وأهم متصفح عرفه مستخدمي الإنترنت ، ومع أنه يتنافس مع عدد هائل من المتصفحات وكلها مجانية ، إلا أنه يعتبر الأفضل في الأمن والتطوير المستمر ، ودعم جميع المواقع ، وواجهة صديقة للمستخدم

الجدول التالي يوضح من هو موزيلا فايرفوكس مقارنة بمنافسيه .

وهذه الإحصائية من شهر يناير عام 2011

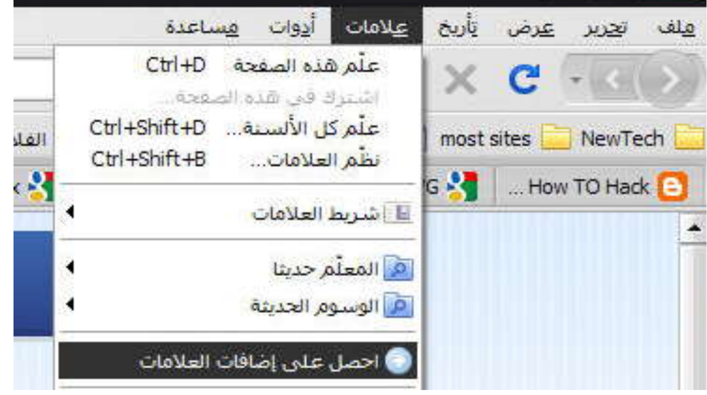
2011	Internet Explorer	Firefox	Chrome	Safari	Opera
January	26.6 %	42.8%	23.8%	4.0%	2.5%

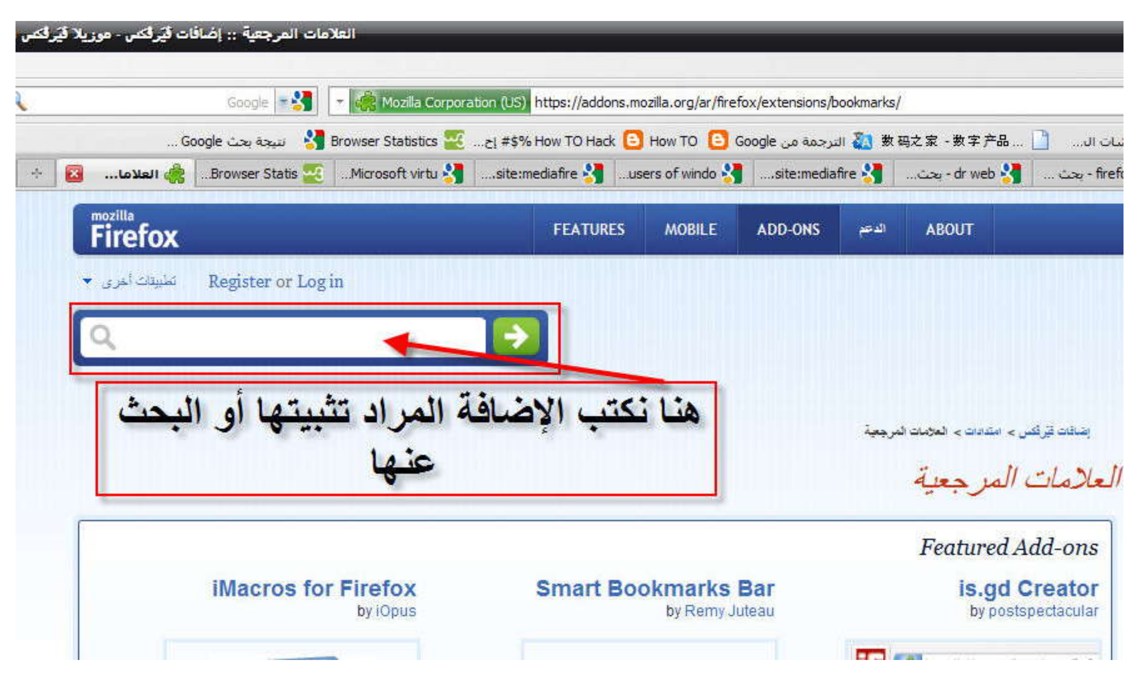
سنشرح بالتفصيل كيف يتم تثبيت موزيلا فايرفوكس ، فور تثبيتك لويندوز جديد خالي من الأخطاء والفيروسات ، وبعد تثبيت للبرامج الأساسية كـ برنامج حماية ، وبرنامج لإدارة التحميل وتسريعه كـ Internet Download Manager

نذهب إلى موقع /http://www.mozilla.com/ar/firefox

ونحمل الإصدار الموجود ، طبعا قد يختلف الإصدار لحظة قراءتك الكتاب ، ولكن سيتم الشرح على متصفح ٣.٦.١٣ وهي آخر نسخة من هذا المتصفح .

بعد تثبيت البرنامج وفور تشغيله نذهب إلى العلامات ثم احصل على إضافة العلامات كالصورة التالية ..





هذا هو الموقع الرئيسي للإضافات وسيتم تحميل بعض الإضافات لعدة أسباب :

الهدف الرئيسي من الإضافات هو التصفح الآمن ، ومنع تام لأي محاولة قد تستهدف تنزيل برمجيات خبيثة خلال زيارتنا لبعض المواقع الغير موثوق بها ، وما أكثرها ..

أما الأهداف الأخرى فتتنوع حسب أذواق المستخدمين ، فالبعض يريد تغيير الجماليات الخاصة بالمتصفح نفسه ، وآخر يريد إضافة كـ الترجمة أو التقاط صور للمواقع ، وآخر يريد حفظ بعض صفحات المواقع بصيغة PDF

كثيرة هي الإضافات ونتمنى أن يتم تصفحها واختيار المناسب منها ، وعدم الإكثار من الإضافات التي لا يدعمها الموقع ، لأنها قد تستخدم من قبل الهاكرز الإجراميين ، فهم نجسوا كل مكان مفتوح ، وللأسف الشديد .

أغلب الإضافات هي من الهاكرز الأخلاقي والذي يهدف لخدمة الناس بشكل مجاني أو بمقابل زهيد يدعوا له من خلال زر Donations أو تبرع .

سيتم شرح كيفية تثبيت إضافة واحدة ، وتتشابه الإضافات فيما بينها إلا أن اغلب المشهور منها يدعم اللغة العربية ومترجم ، وليس جميعها .

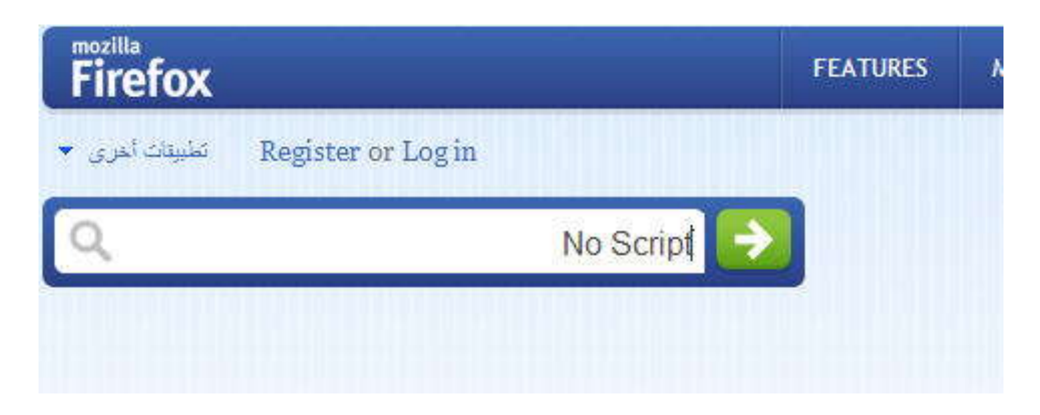
أول إضافة مهمة هي NoScript

هذه الإضافة قد حلت مئات آلاف المشاكل حول العالم ، مثل مشاكل جلوس الأطفال ومنع الإعلانات الغير مرغوب فيها ، والبرمجيات الخبيثة وغيرها الكثير .

تكمن الأهمية المثلى بعدم تشغيل أي كود من شأنه الأضرار بجهازك سواء كان هذا الكود حميد أو خبيث ، وأنت لك الحرية في اختيار من تسمح لهم ، ومن لا تسمح لهم ، أكاد أجزم بأن هذه الإضافة بمثابة جدار ناري للتصفح ، وهي مهمة جدا في للجميع حيث تمكنهم من مراقبة فعالة وقوية للصفحات التي يتم تصفحها يومياً .

طرق تثبيت الإضافة **NoScript** وتثبيت باقي الإضافات مطابق تماما لما سيتم شرحه .

نذهب لموقع الإضافات الرسمي داخل موقع الفايرفوكس

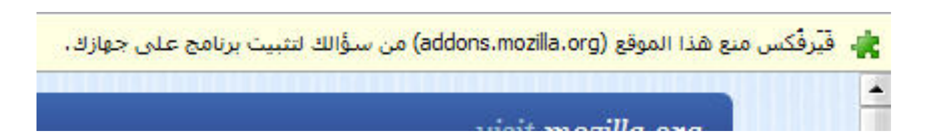


نكتب اسم الإضافة **NoScript**

ثم نتابع كـالآتي ::



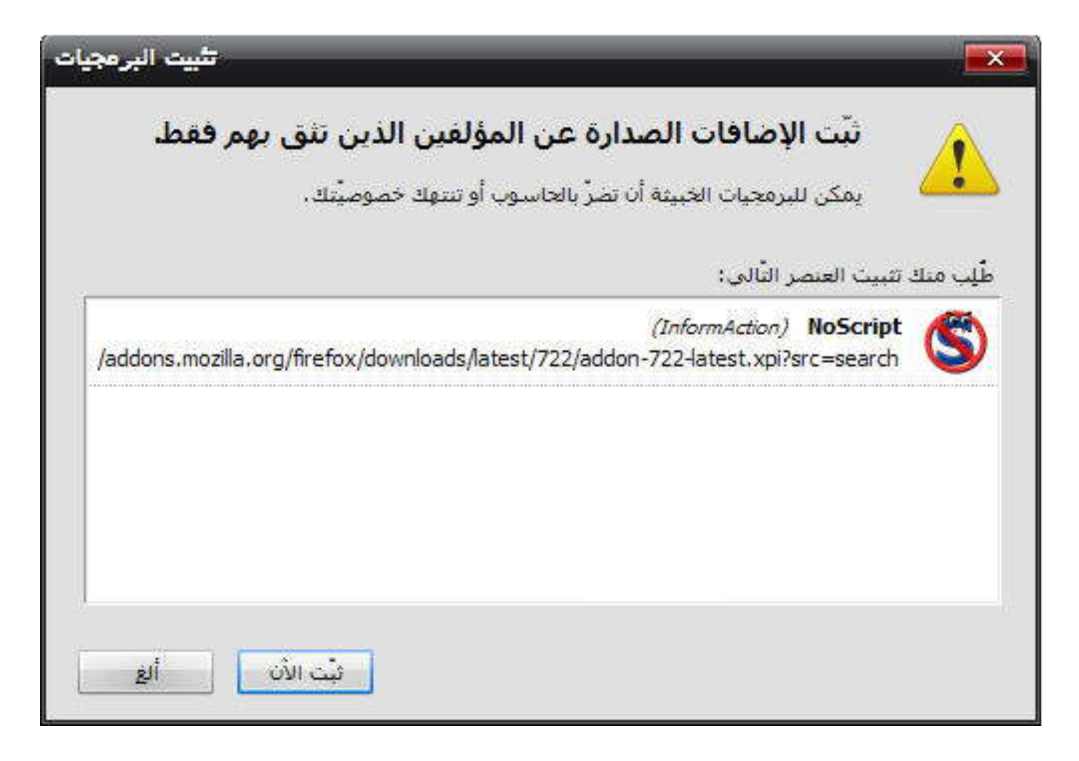
ثم نتابع ::



نضغط على الزر في نهاية السطر الظاهر بالأعلى والمكتوب عليه (اسمـــح)



ثم يظهر لنا التأكيد التالي ، وسيظهر في كل إضافة نحاول تثبيتها ، فالرجاء الحذر من هذه الرسالة فقد يتم اختراقك ، بشاشة كالذي سنستعرضها ، إقراء ما تحاول أن تخبرك به ، وراجع وثوقك في الموقع الذي أظهرها لك ..



طبعا تضغط زر (ثبت الآن)

أعد تشغيل فايرفوكس بعد الانتهاء ، وفور تشغيل ستلاحظ ظهور رمز الإضافة أسفل يسار المتصفح ، وفور دخولك أي موقع يشغل سكريبتات ، وهي ممكن أن تحتوي على برمجيات خبيثة .

إذا كان الموقع مشهور وموثوق فيه كاليوتيوب أو قوقل أو هوتميل وياهو ، فنسمح بالطبع لأنها مواقع في غاية الأمـــان .

تابع مالذي سيحدث عند دخول موقع قوقل مثلاً ::



تمر بالماوس فوق رمز الاسكربت فتظهر الخيارات بالسماح ، أو السماح المؤقت ،لا حظ أننا سنضغط على زر اسمح من موقع قوقل ، وهذا معناه انه سيتم دائما السماح لموقع قوقل بتشغيل سركبتات ، ووضعه في قائمة المواقع الموثوق فيها ، أما إذا دخلنا موقع آخر مشبوه ، فالوقـاية دائما خير من العلاج ، تجنب تشغيل السكربتات في أي موقع تشك بنسبة ضئيلة أنه يحتوي شيء .

وسندرس معاً كيف يتم معرفة المواقع الموثوقة ، والمواقع الغير موثوقة ، والتي سنتجنب تشغيل السكربتات فيها ..

نتابع تثبيت الإضافات التي سنحتاجها خلال تصفحنا ،

سنحتاج إضافتين لنعرف أكثر عن المواقع الموثوقة ، وهي إضافات ذات انتشار عالمي كثيف ، حيث يقوم بتطويرها إدارة شبابية رائعة تهدف لجعل الإنترنت عالماً رائعاً خاليا من مشاكل التجسس ، والأخطاء الغير مبررة والتي يتم إنشاءها عادة من قبل أطفال الهاكرز والذين لم يتخصصوا في شيء أكثر من الغباء ، حيث يمضون الساعات الطوال في تعلم اصطياد مستخدمي الانترنت وبالتالي اختراقهم وتهديدهم أو التمتع بالتجسس عليهم وعلى حياتهم الشخصية ، يمضون الوقت الطويل في قراءة سجلات المحادثات ، أو تصفح رسائل البريد أو متابعة المايكروفون والكاميرا وغير ذلك الكثير من أعمال لا تخدم إلا أمراضهم النفسية التي صاحبتهم خلال حياتهم .

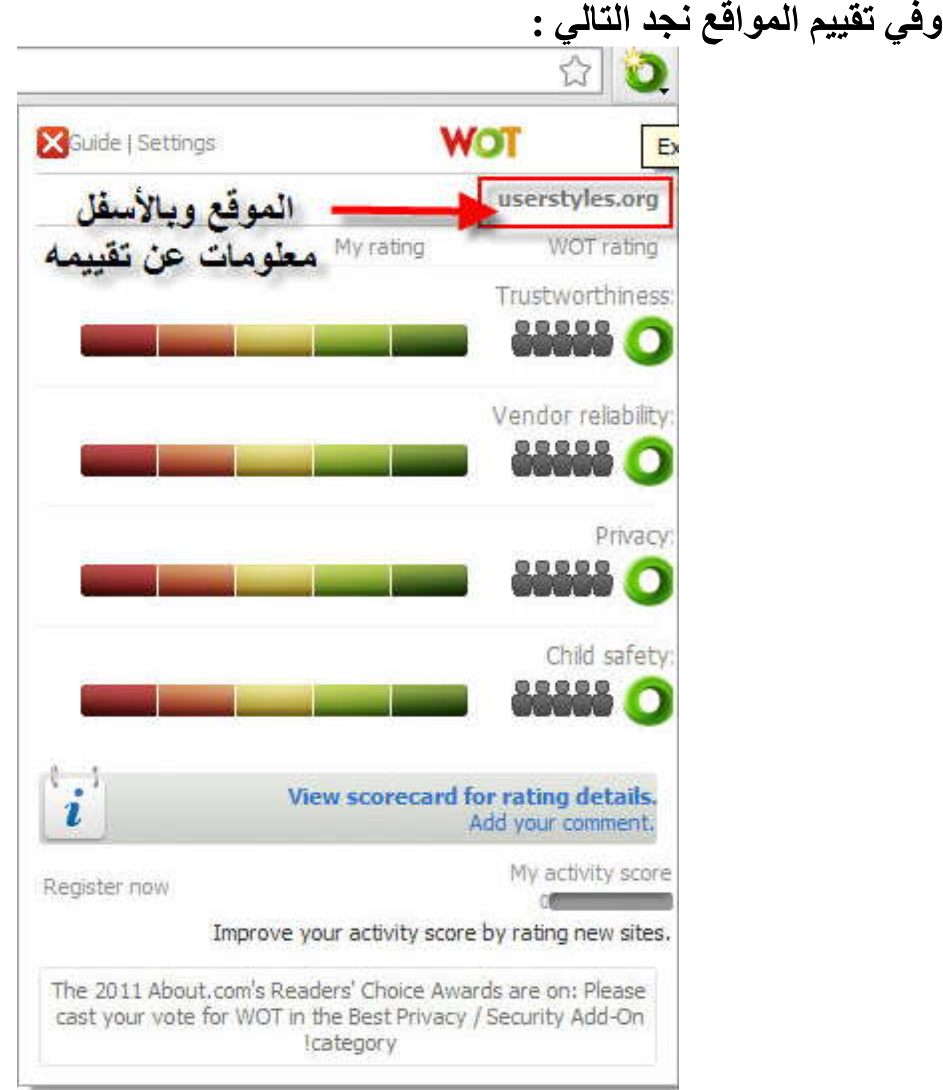
الإضافة الأولى وهي لمعرفة الموقع الذي نتصفحه هل هو آمن ، هل قام أحداً من الخبراء بتصفحه ورؤية أخطاءه ، وما إلى ذلك

اسم الإضافة :: wot

Web of Trust - Safe Browsing Tool



وفي تقييم المواقع نجد التالي :



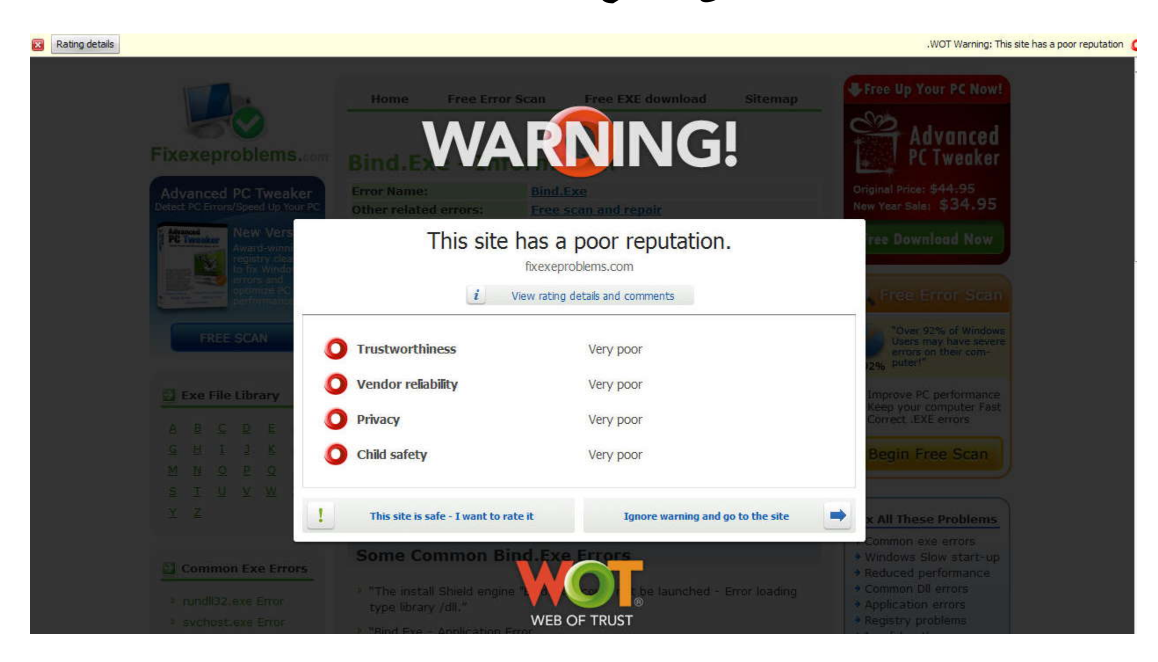
كما تلاحظون فتحنا إحدى الموقع ، إذا مررنا بالماوس فوق إشارة الإضافة سيعطينا تلخيص وتتضمن حالات المواقع بالآتي ::

Excellent موقع ممتاز وموثــوق به .

Good موقع تم تقييمه على أنه آمن ولكن بنسبه أقل .

 **عند ظهور هذه العلامة فمعنى ذلك لا يوجد إحصائيات كافية لتقييم الموقع .**

أما إذا ظهرت هذه الشاشة على الموقع المراد تصفحه ::



فهذا يعني أن الموقع تم تقييمه ، ويعلمك بأنه موقع سيء جداً وله سمعة سيئة ، و إياك وتصفحه اخرج من الموقع فوراً ولا تقم أبداً بتجاوز ما يخبرك به ، لأنه دقيق إلى حدا ما حيث لا يقوم بالتقييم هواة يقيمونه من خلال الشكل أو الظاهر ، بل قد يكون من قيم الموقع أحد ممن ضرهم الموقع ، أو حاول ضررهم ..

الإضافة الثانيــة ::

اسم الإضافة :: LinkExtend

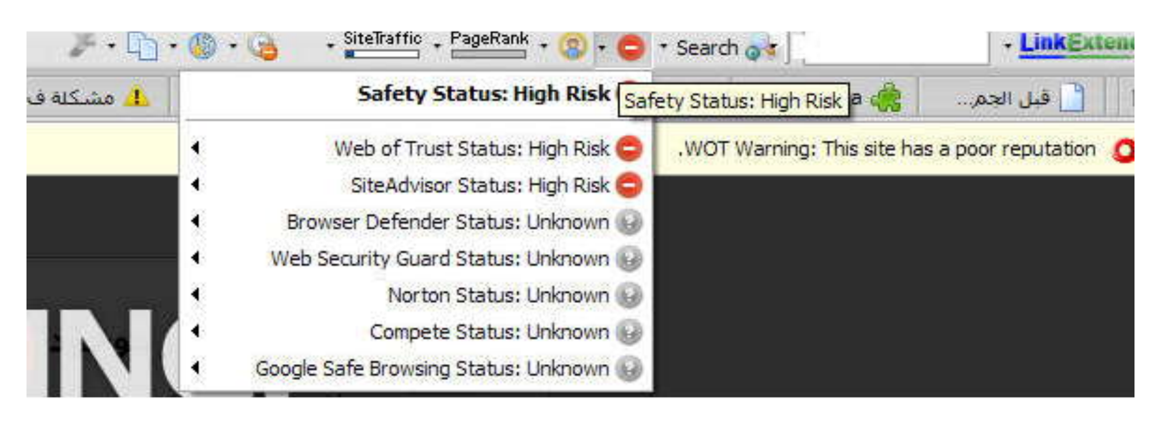
LinkExtend - Safety, KidSafe, Site Tools

بعد البحث عن الإضافة و تثبيتها كما تعلمنا ، وعند الدخول لأي موقع عادي يظهر الشريط ليخبرنا بالتالي ::



لمعرفة المزيد عن الموقع ، ننقر فوق علامة الصح الذي سيتلون تبعا للموقع الذي يتم تصفحه ، وهو في هذا الحالة لا يعتمد على تقييم ، بل يفحص قاعدة بيانات المواقع التي صنفت هذا الموقع على أنه خطر .

عند الدخول لموقع مصنف على أنه خطر سيحدث الآتي ::



وكما نرى فقد تم منع الموقع بواسطة الإضافتين عن المواقع

فكلا الإضافتين قد صنفت الموقع على أنه في غاية الخطورة ، موفقين إن شاء الله في التصفح الآمن ، وفقكم الله في التصدي لأعداء الإنسانية وحماية أنفسكم وأطفالكم في المستقبل من هؤلاء المحسوبين على البشر .

طبعاً هناك آلاف الإضافات التي يتم تجديدها لا تعتمد على الكتاب بعد مرور عام من الآن إذا لم تنزل طبعة ثانية لعام ٢٠١٢ أو قبل ذلك ، دائماً كن متفاعلا مع التطورات وابحث عما يفيدك ويطور خبرتك في حماية نفسك ، فما ذكرناه الآن خلال هذا الكتاب قد يتم تجاوزه بعد أشهر أو حتى أيام ، ولكن هناك الكثير من المواقع العربية والأجنبية المحترمة والتي تعطيك المعلومة في كثير من الحالات بدون أدنى مقابل ، أستغرب حقاً أن ديننا يفرض علينا عدم كتم العلم ، ونشر المعرفة والقراءة ، وتطوير الذات وغير ذلك من الأمور الجيدة إلا أننا اليوم أكثر الأمم تخلفاً ، حيث مجموع المواقع العربية التي تعطيك المعلومة دون مقابل تكاد تساوي عدد مجموع مواقع طلبة إحدى الجامعات الغربية ، سواء كنا نتحدث عن ثورة الغرب العلمية في أمريكا أو أوروبا أو ثورتها في الصين والدول الآسيوية التي تسير بتسارع تنموي رائع ، يعززه دور حكوماتها ، والشخصيات السياسية

في تلك المجتمعات ، والتي تنقصنا كثيـرا في الوزارات والمؤسسات حتى الخيري منـها !!!!!

وكأنهم يحولون بيننا وبين المعرفة ، ويفرضون على أكثر الشباب البحث عن أعمال بعيدة عن التطوير الذهني ، والرفعة العلمية .

وكأنهم يعرفون أنهم ولو شاركوا في بناء عقولنا ، وكأنهم يشاركون في بناء قبورهم ، يا من تقرأ الكتاب واستفدت منه أرجو أن تمرره لغيرك وتنشر جميع المعلومات التي قد تصل إليها عن طريق الخبرة والتطوير ، وسواء كانت المعلومة خاصة بك أم لم تكن لا تكتمها عن إخوانك ، ولا تكن كـ الذين أعيونا من مقولة منقول ، أو مقولة برايفت (خاص)

صراحة هم يشتركون في أمرين الأول ، عدم مساعدة المعرفة المحتضرة في الدول العربية على الإفاقة من هذا الداء المستمر عبر عقود الجهل والظلام ، ومحاصرتها داخل بوتقة خاصة ، العالم بجميع طوائفه يسعى للعلم والتطوير ومناطحة كل العلوم الإنسـانية ، ونحن نفكر في هل هذا الموضوع منقول ، أم لا !!!!!

بعض الإحصائيات تقول أن العالم يتطور أسبوعيا إلى الضعف ، ونحن نفكر هل أخبئ المعلومة التي اكتشفتها تواً أم لا ..

وتمر الليالي الطوال في المنتديات العربية ، بين جاحد لمن علم ، وعالم بما لا يعلم ، صدقوني أن أغلب بخلاء المعلومات هم أساسا أحضروا جل علمهم من مشاركات الكثيرين من العرب ، والأجانب وغيرهم .

وقد يكون قد سمع المعلومة في إحدى المواقع الأجنبية ، وترك كلمة في إحدى مواضيع الاستفهام وما أكثرها قائلاً برايفت .

إن كان هناك جمعية خيرية واحدة لما لا تتبنى مشروع للرد على جميع الاستفسارات التي صرخت ولم تلقى إجابة ، لما لا تتمنى إحداها مشروع لتوزيع مثل هذا الكتاب بشكل مجاني على من يحتاجه فعلاً ، تجد الكثيرين يتمرغون في أقسام الترفية ، وآخرين في السياسة وهم بعيدون بالطبع عن فهم أصلا معناها .

لما لا نجدهم وهم ذو علم في أقسام الاستفسارات ومساعدات الأعضاء وغير ذلك الكثيـر ..!!

حسبنا الله ونعم الوكيـل ..

الدرس السابع : الفرق بين

أنواع الملفات والمواقع

لعل من أهم ما ستتعلم من هذا الدرس كيف تفرق بين أنواع الملفات التي يجب أن أحذر عند تشغيلها ، وما هي الملفات التي لن تقلق عند تشغيلها ، يجب أن تعرف في البداية أن الحاسب لا يهمه اسم الملف ، فكل الأسماء عنده سيان إذا كانت تستوفي الشروط أي لا يمكن أن تحتوي على إحدى الرموز

لا يمكن أن يحتوي اسم ملف على أي من الأحرف التالية:
\/:*?"< >|

إذا فكيف يميز أن هذا الملف صورة أو فيديو أو برنامج أو أي شيء آخـر ..

يعرف من خلال الامتدادات Extensions

وهي ملحقات أسماء الملفات التي يتم تعريف الكومبيوتر بواسطتها ما هو نوع الملف ، وما هو البرنامج المخصص في الجهاز لتشغيل هذا النوع ، وإن لم يتواجد أي برنامج فتظهر لك القائمة التالية ::



وهذا معناه أن جهازك لا يوجد به برنامج لتشغيل هذا الامتداد ، والظاهر بوضوح أمامنا أننا أمام امتداد hmh

وهو امتداد وضعته لأكمل الشرح فقط وليس له وجود على حد علمي البسيط ☺ إذاً نلخص ما تعلمناه حتى الآن بالتالي :

أن نظام التشغيل (ويندوز) لا يهمه إلا شروط معينة في اختيار الاسم ، ذكرناها سابقاً .

وأنه أيضا يفرق بين أنواع الملفات من خلال اللاحقة أو الامتداد أو إلي ثقافته عنقليزي الـ extension

الامتداد غالبا ما يتكون من ثلاث أحرف قد تزيد أو تنقص حسب البرنامج الذي تم إنشاؤه بواسطته .

هناك بعض الامتدادات التي يمكن صنعها بنفسك ، لا أريد التثقيل عليكم بالشرح ، المهم أن أي امتداد نستطيع تعديل البرنامج المخصص لتشغيله أيضاً .

فمثلاً ::



كما هو واضح الملف عبارة عن مستند نص ، ويتم فتحه بواسطة برنامج افتراضي مع الويندوز يسمى Notepad ولكننا نستطيع فتحه بأي مستعرض ملفات نصية آخر إذا توفر لنا غيره (:

يفصل بين اسم الملف والامتداد نقطة (.) ، وفي غالبية إصدارات أنظمة التشغيل يتم عدم إظهار الامتداد للمستخدم حتى لا يتم تنغيص حياته كلما أراد تغيير الاسم وبإمكاننا إظهار امتداد الملفات من خلال الذهاب إلى ::



كما هو ظاهر نذهب لمستعرض الملفات ، ونضغط (أدوات)

ومن ثم (خيارات المجلد) ، فتظهر القائمة التالية ..



تزيل علامة الصح من أمام (إخفاء ملحقات الملفات لأنواع الملفات المعروفة) وتضغط موافق ، فتصبح الملفات أمامك كل ملف بعد الاسم الامتداد الخاص به .



كما هو أمامك كل ملف يظهر في آخره امتداده ، تذكر عند إعادة التسمية لا تنسى أن تغير الاسم فقط ، ولا تشطب اللاحقة معه !!

وحتى لا أفاجئك بعد ذلك اكتشف الهاكرز حديثاً جدا ثغرات تمكنهم من الاختراق بأي صيغة حتى صيغ الصور والفيديو وغير ذلك ، وأهم هذه الثغرات ::

اسم الثغرة :: **Buffer OverFlow**

وهي ثغرة مصابة بها أكثر البرامج ، تعمل على الثغرة على رفع البرنامج لأعلى مستوى له مما يحدث خللاً معيناً يسمح بتشغيل ملف معين يتم دمجه ببرنامج خبيث للعمل داخل جهازك دونما تشعر ، وتعتبر هذه العملية أحدث طرق الاختراق .

إذن في ماذا سيفيدنا معرفة أنواع الملفات ..؟؟

يقولون إذا أردت أن تعالج خطئاً ما يجب أن تبحث عن المصدر والمسبب ، فما من مريض يتصل بالمستشفى فيوصفونه الدواء ، لذا وجب عليك قراءة هذه المعلومات البسيطة والتي ستخبرك بأوائل خطواتك في تطوير القدرة الشخصية في مواجهة أي شيء قد يطرأ على البيئة البرمجية التي تعمل نم خلالها ، و ما شاء الله أصبح محرك البحث العالمي قوقل يستخدم من قبل رجالات المخابرات (طبعا في الدول العربية بس يمكن !!) المهم أن المعلومات تتكاثر يوميا وتتطور ويجب أن تطور معرفتك بعد ما ستتعلمه بإذنه تعالى من خلال هذا الكتاب البسيط .

يجب أن تتعلم في البداية أن هناك امتدادات معينة تتعامل مع الويندوز مباشر ، أولا تحتاج لمترجم لتشغيلها .

بمعنى أن الصور تحتاج لمستعرض الصور ،

ملفات الفيديو تحتاج لمشغل الفيديو ،

ولكن البرامج مثلا لا تحتاج واسطة أو مشغل لها لتعمل ، بل تعمل فور الضغط عليها لأنها تنفيذية ، إذ أن نظام التشغيل يقرأها وينفذها فور تشغيلها .

لذا هناك امتدادات خطيرة يستخدمها عموم أطفال الهاكرز وهي ::

Exe وهو امتداد البرامج الرئيسية .

Scr وهو امتداد شاشات التوقف .

Pif , bat , com وجميعها امتدادات برامج كانت تستخدم في الدوس أول نظام تشغيلي

Vbs امتداد تشغيل كود فيجوال بيسك سكربت

Shs وهو امتداد كائن انتقالي

المهم عليك بعد معرفة ما سبق أن تحذر مما تقوم بتحميله من الانترنت ، ولا تحمل البرامج من المواقع العامة ، بمعنى لا تحمل من موقع يسمح للمسجلين فيه بتحميل كل ما هب ودب ، أمثال مكتبات تحميل الأفلام فأغلب البرامج التي يتم وضعها مسروقة من منتديات أجنبية أو مواقع مشهورة ، يستخدمها الهاكرز في نشر الفيروسات الخاصة بهم .

وهذا يدفعنا للجزء الثاني من هذا الدرس وهو درس التفريق بين المواقع .

صحيح أننا استخدمنا الفايرفوكس في حماية أنفسنا من المواقع المصنفة على أنها خطيرة ، وجب أن نحذر أيضا أن هذا لا يكفي إذ يقوم بعض الأشخاص بإغرائك فتح مواقع من صنعهم إما برسالة بريد إلكتروني أو عبر الشات أو غير ذلك ، وهذا يوترك ولا تستطيع التفريق بين المواقع الموثوقة وغيرها .

لذا سنتناول هذا الجانب في هذا الجزء قائلين أن هناك عدة أنواع من مواقع الانترنت .

النوع الأول ::

موقع ضخم يشرف عليه مجموعة كبيرة من المبرمجين والخبراء والاستشاريين ، ولا يقوم وضع البرامج إلا بعد فحصها وتدقيقها ، ومن ثم تقديمها للمستخدمين كـ موقع التحميل الشهير

/http://www.download.com

وموقع

/http://www.softpedia.com

وهي مواقع في قمة الوثوق ، وتستطيع تجولها والتحميل منها دون أدنى شك بإمكانية احتواء بعض البرامج على إحدى الاكواد الخطيرة ..

النوع الثاني ::

موقع ضخم ولكن لا يتم الإشراف إلا من قبل فريق صغير جداً ، في غالب الأحيان مجموعة بسيطة من الشباب تم بواسطتهم تكوين الموقع بهدف التربح السريع من خلال الضغط على الإعلانات كـ مواقع عربية مشهورة ::

/http://myegy.com

/http://www.arabseed.com

/http://www.arablionz.com

وغيرهم الكثير ، وهم في الغالب للأسف الشديد لا يتم التدقيق فيهم على البرامج التي يتم تنزيلها للمستخدمين ، وهي في الغالب منسوخة من مواقع أجنبية تم دمج تلك البرامج أو باتش تفعيل البرنامج بأساليب غاية في الدقة و الإتقان ، وبأيدي خبراء ومهرة في فنون الهاكرز بهدف جلب أكبر أعداد الضحايا .

النوع الثالث ::

موقع أو مدونة خاصة لإحدى الهواة ، طبعا لا نجمعهم كلهم في قفص اتهام واحد من المؤكد جداً أن يكون من بينهم الكثير من الأشخاص الخدومين ، والذين يريدوا نشر المعرفة والبرامج الجيدة والجديدة ، إلا أنهم وفي الغالب يفتقروا مهارات الفحص قبل النشر ، ويصبحوا وللأسف أداة بيد الهاكرز لنشر المزيد والمزيد من خدعه التي تنطلي على الكثيرين ، نتيجة الوعي البسيط في طرق فحص البرامج

والتأكد من خلوها جميع أنواع الفيروسات ، سواء من صاحب الموقع ، أو حتى ممن حمل هذه البرامج ..

ولن أطرح هنا أمثلة إطلاقاً ، إلا أني سأوضح كيفية اكتشاف مواقعهم .



كيف عرفنا أن هذا الموقع قد يحتوي على برامج قد تكون مدموجة بأكواد خبيثة ،

تعالوا نحلل العنوان ::

نقسم العنوان إلى قسمين

القسم الأول ما بعد //:http وحتى النقطة http://e5terq.

القسم الثاني ما قبل / الثالثة وحتى النقطة blogspot.com/:

طبعا شيئا فشيئا ، سيتكون لدينا قاعدة بيانات هائلة ، نتعرف من خلالها بمجرد النظر هل هذا الموقع تابع لموقع آخر أم لا ، أما موقع BlogSpot فهو موقع يقدم خدمة المدونات المجانية ، وجدير بالذكر أن نذكر أن المدونات بلغ عددها اليوم أكثر من ١٥٠ مليون مدونة .

المهم إذا أردت أن تعرف أكثر ما من ضير أن تأخذ القسم الثاني ، وتكتبه وحده في شريط عناوين المواقع ، وتدخل الموقع وترى هل يقدم خدمة صفحات مجانية أم لا ، وللمزيد تستطيع البحث أكثر عن الموقع وترجمة الصفحات عبر قوقل وما إلى ذلك ، حتى تصل لفهم أكثر عن خدمات هذا الموقع أو ذلك ؛ جدير بالذكر أن اغلب المواقع العالمية هي مواقع لأمريكيين لأننا يعنينا اللغة الانجليزية أكثر من غيرها هناك الكثير من المواقع التي تقدم خدمات ضخمة جديدة ولكنها بلغات أخرى كاليابانية والصينية والروسية وغيرهم .

أرجو أن يحاول من له وقت أن يظهر محاسن بعضاً منها ، ويحاول نشر هذه المواقع على الصعيد العربي ، مما سيشكل ضغطا على المسئولين العرب الذين أصبح شغلهم الشاغل وضع عناوينهم في الفيس بوك أو تويتر أو غيرها من المواقع الاجتماعية لمحاولة التأثير على الشباب العربي ونشر تلك المواقع ، لا منافسة هذه المواقع بهدف إنشاء مواقع عربية تدعم المصالح العربية والتطلعات الشبابية بمستقبل عربي أفضل .

الدرس الثامن : تجميـد النظام

يقصد بتجميد النظام ، هو وضع النظام مجمد بحيث لو قمنا بتعديل أو حذف أي شيء بمجرد تشغيل الويندوز يعود كل شيء إلى وضعه المجمد ، وهو برنامج يتم تثبيته وسهل جدا لا يحتاج لشرح بالصور ، ولكني سأشرحه !!

طبعا التفسيرات ستتضح الآن ، واعذروني أحاول تبسيط المعلومة قدر ما أستطيع ، وإن شاء الله سنتناول بالتفصيل كيفية الحصول على نظام مجمد .

السؤال الأول :: ما الهدف من تجميد النظـام ..؟؟

الحصول على نظام ملفات معين ، وحينها يتم السماح للأطفال أو الزوار أو أيا يكن باستخدام الجهاز بشكل كامل ، دون خوف من إمكانية حذفهم للنظام أو اختراقه ، أو تثبيت أي برمجيات خبيثة للتجسس والكثيـــر ..

السؤال الثاني :: كيف نجمد النظام ..؟؟

يتم تجميد النظام بواسطة برنامج يسمى DeepFreeze

أو أي برنامج آخر له نفس الخصائص ، وهي برامج تصنع نقطة لكامل ملفاتك الحالية ، وفور إعادة تشغيل جهازك تتم مقارنة الصورة الحالية بالصورة الأصلية المجمدة ، وإعادة الأصليـة ..

السؤال الثالث :: هل أستطيع تثبيت أي برنامج بعد تثبيت برنامج التجميد ..؟؟

تستطيع ذلك ، إذا كنت مديراً للجهاز ، بمعنى هذا البرنامج سيسمح لك بإنشاء كلمة مرور معينة له ، وبمجرد محاولة التعديل على خصائصه بإيقافه مثلا يسألك عن كلمة المرور ويجب كتابتها حتى تتمكن من إيقافه مؤقتا لتثبيت برنامجك ثم العودة لحالة التجميد ، ولكن يجب إعادة التشغيل في كل مرة توقف أو تشغل عملية التجميد ..

السؤال الرابع :: ما رأيك الشخصي بهذا البرنامج ..؟؟

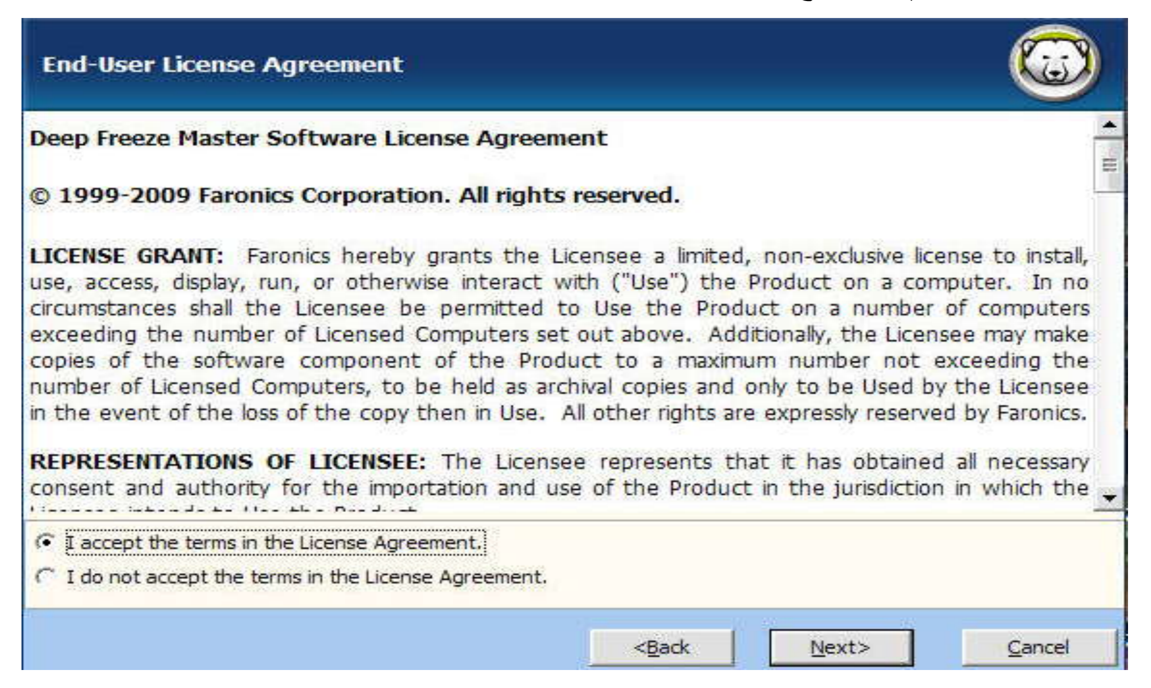
هذا البرنامج يصلح للأطفال ، أو في جهاز عام ولكنه يلغي عملية التأثر والتأثير بين النظام والمستخدم ، بمعنى أن الشخص سيعتمد كثيرا على هذا البرنامج ولن يتأثر بمحاولة حماية نفسه ، لأنه يظن أنه آمن كلياً الآن ، فهو فقط سيعيد التشغيل فيعود كل شيء كما كان ، ولكن من وجهة نظري يجب أن يتعرض الدارس للتفاعل مع البيئة المدروسة أيا كانت هذه البيئة ..

سأشرح فقط عملية تثبيته ، ولا أتمنى لأحد يستخدم جهازه بشكل خاص استخدام هذا البرنامج ، هذا البرنامج فقط في حال كان هناك العديد من المستخدمين ذوي المهارات المحدودة في الحاسب

تثبيت برنامج DeepFreeze



طبعا Next كأي برنامج آخر



المفكرة - Key.txt

NKQ7KD4E-MTRZ4606-6NTTCAFX-Z4APSWN4-ZS65BM43

نسخ المفتاح الخاص بالنسخة حتى نشتريها بالعافية لأنا مفلسين ومعناش

Licensing

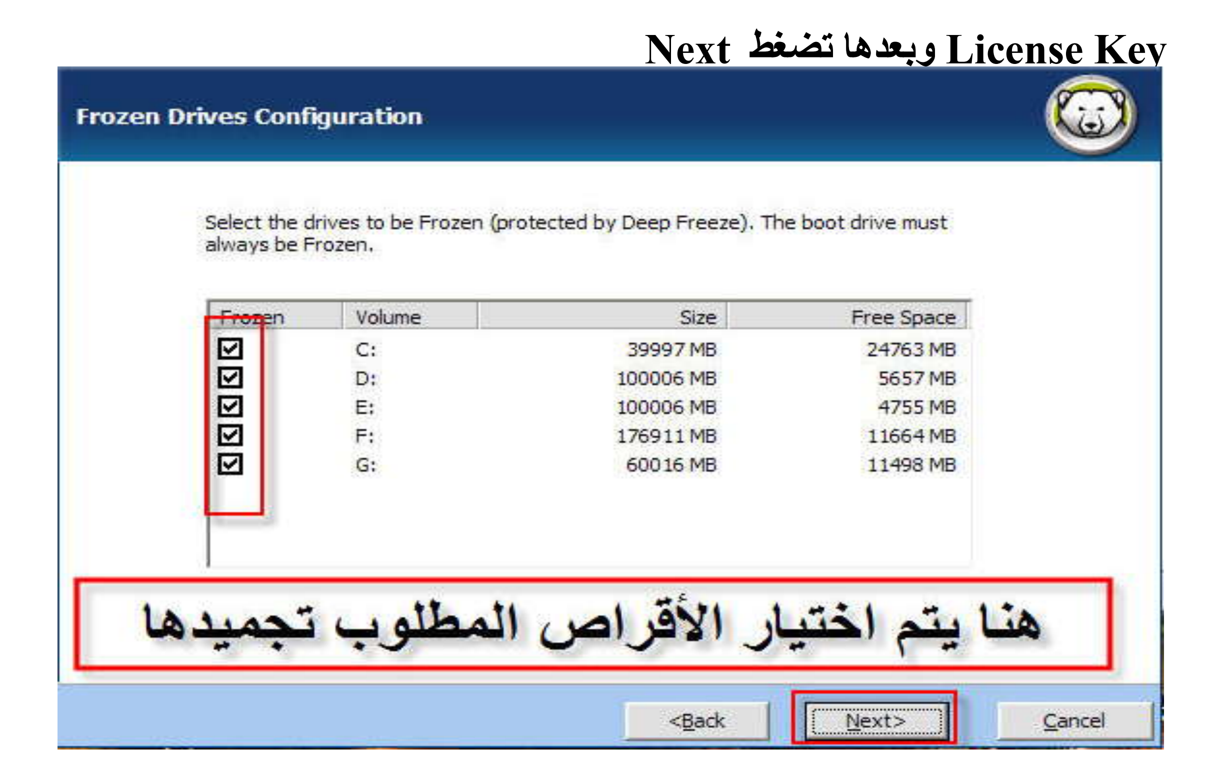
License Key NKQ7KD4E-MTRZ4606-6NTTCAFX-Z4APSWN4-ZS65BM43

Use Evaluation

<Back Next> Cancel

عادة إذا ما تم تحميل برنامج **DeepFreeze** من إحدى المواقع التي تسمح بعرض مفاتيح تسجيل البرامج ستجد مستند نص فيه مفتاح تسجل المنتج ستدخله في خانة

License Key وبعدها تضغط **Next**



بعد إعادة التشغيل ستجد أن كل شيء تم تجميده ، وستظهر لك قائمة تخبرك بوضع كلمة سر افتراضية للبرنامج ، إذا لم تدخل كلمة سر سيستطيع أي مستخدم استخدام البرنامج وإيقافه عن العمل وقتما يريد .

إذا لم تظهر لك القائمة اضغط

Ctrl+Shift+Alt+F6

البرنامج من الداخل سهل جدا ،



وبهذا نكون قد وصلنا إلى نهاية هذا الدرس

وفقنا الله وإياكم إلى ما فيه الخير والصلاح .

وعدل أمورنا وأمور الإنسانية جمعاء .

ملاحظة :

تم تخطي تجميد النظام من قبل الهاكرز في بعض إصدارات البرنامج هذا أو غيره ، لذا أرجو الحذر الشديد عند تثبيته أو الاعتماد عليه .

القسم الثاني : فنون فحص وحماية النظام

نبذة عن القسم ::

لعل من أبرز ما يقلق صاحب البيت حمايته من شتى المخاطر التي قد تلحق به ، وأولى هذه المخاطر التجسس ..!!

لا يستطيع أحد أن ينام وهو يعلم بأن جاره أو حتى أقرب الناس إليه قد يستطيع أن يشاهده أو يعبث بأغراضه الخاصة جداً ولا يحرك ساكناً .

هذا الساكن الذي نأمل أن نحركه في كل من يقرأ الكتاب ، مغيرين طريقتنا في أي تكنولوجيا تقع في أيدينا ، يجب أن نفحصها جيداً ونرى ما لها وما عليها ، ويجب أن يقوم مهندسو العرب بإصدار ملخصات دورية عن جميع الأجهزة التي بدأت تخترق كل البيوت ، ولا يعرف لماذا وكيف ، ومن أين ..!!

كل هذه الأسئلة يستطيع أي طفل متابع لأحداث العالم أن يجيب عليها .

أما لماذا .. فالجواب

لم يكن يوم من الأيام حلم للإنسان أكبر من حلمه من التمتع بخواص ضخمه تتيح له التجسس على أي شيء أينما كان ، استطاع هذا الإنسان أن يحقق حلمه بالتجسس المباشر أوائل التاريخ باستراق السمع أو البصر ، ثم مع ظهور التكنولوجيا حديثاً كان لا بد من تنظيمها جيداً ، وعدم وصولها لأيدي ضارة قبل وصولها للسفاح الرئيسي أولاً ، فمن يملك المعلومات يملك العالم ، بدأ حلف التكنولوجيا في التشكل داخل دولة تم تعظيمها وتمجيدها لأنها تملك شيئا واحداً أسس لامتلاك ملايين أو بلايين الأشياء بعده ، وهذا الشيء هو المعلومات ، استطاعت الولايات المتحدة الأمريكية ، وفي ظل اهتمام المنافسين المتخلفين في الصناعات العسكرية أن تؤسس أجهزة عملاقة لها خبراء في شتى المجالات أهم هذه المجالات هو المجال التكنولوجي ، والذي خرج علينا الآن بتطوير يليه تطوير ، هذه التطويرات المتسارعة كانت موجودة من عشرات السنوات ومصنفة على أنها في قمة السرية ، ولم تقم أي من الدول خصوصا المعادية لأمريكا بإدارة أي مشروع تطويري خاص ، ليس هذا فحسب كانت المعلومات تصل لأمريكا وتستهدف من تريد بمشاركة بعض الدول التي أيدت التطلع الأمريكي ، والتزمت بالخطط الأمريكية في السيطرة على العالم معلوماتياً ، ومن ثم اقتصادياً ، فالمعلومة

هي الأجدر والأولى بالظفر بها ، تميزت هذه الإدارة بتفخيم القادة حتى بعد تقاعدهم ، بل وفرت لهم أضخم وأفضل أساليب الاستجمام في العالم الحديث ، حيث ابتكرت استرجاع المعارك والحروب في صالات ضخمة خاصة ، وبعدها حولت بعض تلك الصالات إلى أماكن سياحية يستطيع البعض ومن ثم الكل دخولها .

كانت هذه الخطة الحكيمة و مازالت حية ونراها حتى الآن ، استخدمت أمريكا في عمليات السيطرة على معلومات وتكنولوجيا العالم الكثير من الآليات ابتداءاً من عمليات الملاحقة والاغتيال ، مرورا بالعقوبات الاقتصادية واختلاق الكوارث والأزمات السياسية وغير ذلك الكثير .

ما يؤكد هذه النظرية هو خروج جميع الابتكارات الحديثة من حظيرة وزارة الدفاع الأمريكية ، فالعالم الآن يؤكد على أن أكثر وسيلة تكنولوجية تم ترويجها في العالم هي بالأساس مشروع لوزارة الدفاع الأمريكية تبنته في الستينات ، وأخرجته للعالم في بدايات التسعينات ، هذا المشروع التكنولوجي الضخم (الإنترنت) ، والذي بواسطته ستستطيع أمريكا التجسس على جميع المعلومات في العالم ، بل ومراقبة الجميع وقتما تحتاج سمعياً وبصرياً وحتى حسياً .

لم تكتفي أمريكا بهذا ، فالتكنولوجيا ستكون مركونة في إحدى أركان المنزل ، من خلال حاسوب قد يتم إطفاؤه في أي لحظه أو فصل التيار الكهربائي ، طورت المشروع شيئاً فشيئاً حتى وصلت لتصغير الآلة التي يستخدمها المستخدم لتلقي الإنترنت ، فكان في البداية اللابتوب ، ومن ثم جاء الاكتشاف الكبير في دمج أضخم مشروعي تجسس في العالم معاً ، الهواتف النقالة والإنترنت بكافة ما يحتوي من إمكانيات جبارة ، كان لا بد من الاتفاق مع شركة عملاقة مولودة فعلياً حتى يتم استساغ اللقمة الأمريكية الجديدة العالم ، وتأتى هذا من خلال شركة آبل العالمية ، والتي كان لها السبق في خروج وليدها وانتشاره عالمياً ، وما من أحد على مستوى العالم يعارضني القول أن نوكيا تسير نحو اندماج أمريكي متوقع ، فنوكيا والتي لم تكن يوماً ليست أمريكية استطاعت أن تخفي هذا علناً ، لأننا ذكرنا أن المعلومة وأمنها بيد أمريكا ..!!

زاد إذن حيز التجسس ووصل إلى ما وصل إليه اليوم ، وأذكر أن جميع التقارير التي قيلت والتي للأسف لم تتناقل كما أراد من وزعها ولم تصل إلى جميع مستخدمي الهواتف الذكية ، حتى الاسم تفننوا فيه لإغواء المستهلكين الذين أكثرهم مستهدف إن لم يكن جميعهم ..

ليس هذه الأسباب وحسب ، وإنما استهدفت أمريكا اليوم البعض بالكل ، فـ جميعنا يعلم تواطؤ بعض القيادات في كثير من الدول مع أمريكا وحلفاؤها ، مما يزيد من تشتت المواقف المعارضة ، ويقلب أي محاولة من شأنها تغيير اللاعبين الأساسيين في الملعب الدولي الضخم .

جعلت أمريكا شغل الأمم الآن في الغالب التطور الاقتصادي ، ولقمة العيش والاقتداء بالغرب ، فتحولت أحلام الشباب بفعل الإعلام المتأمرك من أحلام القوة والحياة من أجل الهدف الأسمى وهو البلد الأم ، إلى أحلام وصول الغرب وخاصة أمريكا ، والتنعم بخيراتها والتلذذ في ما وصلت إليه .

وهذا هو حال كل المظلومين في العالم والذين يرون أن الأقوى هو الأجدر بالاقتداء ، وإذا اقتدينا بهم تناسينا أول حلم لنا على ظهر البسيطة ، بل ونسينا أنفسنا في بحر لا يعرف تخطيه أحد ، فمن يغرق فيه لن يخرج إلا حين يأتيه اليقين ، أو قبلها بقليل .

يقول سبحانه وتعالي ::

{ وَلا تَكُونُوا كَالَّذِينَ نَسُوا اللَّهَ فَأَنسَاهُمْ أَنفُسَهُمْ أُوْلَئِكَ هُمُ الفَاسِقُونَ}

[الحشر : ١٩]

للمزيد أرجو الإطلاع على مقال رائع ، وحكيم جداً للأستاذ الدكتور :: عبد الكريم بكار

في موقع صيد الفوائد

http://www.saaid.net/Doat/bakkar/023.htm

أرجو أن أكون قد وضحت صورة ، غائبة عن البعض .

وأرجو أن ينتشر من يريد أن يغير هرماً كاملاً لا رأسه فقط .

من أبرز ما يميز العصر اليوم هو التسارع الكبير ، فلم نعد كالماضي القريب ننتظر بضع أيام لكي تصلنا رسالة تحتوي جملة واحدة ، ولكننا اليوم نتعارف مع اللحظة ونرغمها على أن تقف قبل أن تصل آلاف الكلمات بين ملايين الناس على مستوى العالم ، هذه الفلسفة البسيطة كانت لا بد أن تحدث في عصر نسى وأنسى كثيرا من

سكانه ، فأكثر من نصف سكان العالم يعيشون حياة بائسة لا إنترنت ولا أي من مجالات الحياة الفخمة .

إذا كنت تقرأ هذا الكتاب على حاسوب خاص فأنت من ضمن القلائل في العالم المحظوظين جداً لأمرين هما في بالغ الأهمية لقاري هذا القسم :

الأمر الأول : الحال الميسور والذي أعطاك حاسوباً ووقتاً قد تقرأ فيه كتاب من بين آلاف على الإنترنت ، وقد أيضـاً لا تستفيد منه ..!!

الأمر الثاني : التطبيق وهو الوقت الأطول دائماً من القراءة ، حاولت تبسيط المعلومة حتى يستطيع أي شخص تطبيقهـا ، ونشرها أيضاً .

إذن فلنبدأ معاً دروس هذا القسم ، والذي سيخرجك فناناً جديداً ، تحمل خبرة في بناء سور منيع ، وحصن عالي لحماية حاسوبك ، وحاسوب من تحرص على حمايتهم .

حاول نشر الكتاب بكل ما أوتيت من قوة ، ليس لظهور اسمي :)

وإنما للتصريح التالي :

هذا الكتاب للجميـع الحق بنشر المعلومات الواردة فيه ، أو بعضها ، أو سحب أي صورة أو فقرة من الشرح ولكن دون تعديل عليه يبطل بعضاً مما جاء فيه .

للجميع الحق في تغيير اسمي في الكتاب ونسبه لنفسه ، أو اقتطاف جزء من الكتاب ونشره في أي مكان بدون كلمة منقول أو اقتباس أو أي شيء .

وإني هنا إذ أسمح بهذا ، أسمح به لأن أجري لا أريده من البشر .

وأحتسب هذا الكتاب عند الله كـ صدقة جارية أتمنى أن أنهيها على خير قبل أن يحدث ما يمكن أن يحدث للجميـع .

اللهم اجعل هذا العمل خالصاً لوجهك الكريم .

الدرس الأول : برامج الحماية من الفيروسات

ذكرنا سابقا أن شركات برامج مكافحات الفيروسات أضخم الشركات العملاقة في مجال الإنترنت ، وقد تجد بعضا منها مختلف في اسم البرنامج فقط ، ولكن الشركة الأم هي التي تصدر أكثر من نوع بهدف السيطرة على أكبر شريحة من المستهلكين أو المهتمين بهذه البرامج .

في هذا الجزء سنوجه اهتمام المستخدم العربي خصوصا على أن الانترنت في تنافس دائم بين شركات تهدف لحربة المعلومات والبرامج ، وتحرير القيود الجبارة المفروضة على مستخدمي التكنولوجيا ، والذين هم في غالبهم لا يستطيعون تحمل نفقات شراء العديد من البرامج التي تهمهم ، إما لأسعارها المرتفعة كثيراً ، أو لكثرة هذه البرامج وتعددها في سوق هائل عدده أكثر من ٢ مليار مستهلك .

بمعنى أكثر وضوحاً أننا سنعتمد على البرامج التي يتم شراؤها ، إما من خلال مفتاح تسلسلي سيتم وضعه مع البرنامج ، أو بباتش تفعيلي سنشرح طريقة تشغيله ، وذلك لعدة أمور أهمها :

أننا نؤمن بحرية الانترنت والعدل بين جميع مستخدميه ، ولكن هل سعر البرنامج في أمريكا على سبيل المثال كـ سعره في قرية صغيرة فقيرة في إحدى دول العالم . بالتأكيد المفروض تكون الإجابة لا ، ولكن بالنسبة لهذه الشركات تقسيم سعر البرنامج سيعرض كثير من الشركات للخسارة ، بل وقد يدفع العديد من المحامين في تلك الدول إلى مطالبة تلك الشركات بتعديل الأسعار تماشياً مع الأسعار الأخرى في العالم .

وبين من يعارض ومن يؤيد فكرة كسر البرامج ، ونشرها ، أقول :

أننا كـ عرب يجب أن نحرص على تطوير المخزون الثقافي والعلمي ، وأن ندخل إلى كل المجالات التي قد نشارك في تطويرها ونتنافس في ذلك ، وأن لا نكتفي بذلك ، بل نطور هذا العمل إلى إيمان تام بضرورة تحسين دور الشباب في المدارس والجمعيات الثقافية بهدف خلق مجتمع قوي فكريا وثقافياً ومن ثم ستأتي لا محالة القوه الاقتصادية والسياسية وغيرها الكثير ، وهناك العديد من الأخبار التي تفيد بتوجه لدى بعض الدول العربية على دخول بعض المجالات الحديثة والأتي يجري

التطوير فيها ، إلا أنها وللأسف الشديد تفتقر إلى الدعم الأكبر بهدف إنشاء جيل علمي حريص على تبني فكر التقدم الجماعي لا الشخصي ، بمعنى أن أغلب الأبحاث العالمية تم نشرها على مستوى العالم في عمومها ، إلا أن العرب وحتى اللحظة لا يشتركون مع غيرهم من العرب أنفسهم في طريق التطور والبحث العلمي ، وتجد أن كثير من الخبراء العرب وللأسف الشديد يقدمون خدمات ضخمة للدول الغربية وينسوا أو يتناسوا أن فرق الراتب الضئيل ليس السبب الوحيد في هجرتهم واستمرارهم بخدمة الغرب ، بل هناك الكثير من الأفكار التي تكونت لديهم عن من يستحق التقدم ، ومن لا يستحقه .

وكأننا نحن العرب في وجهة نظر الكثير ممن يعملون في الخارج لا نستحق الخدمة بلا مقابل ، بل نستحق أن نبقى كما نحن ، لأننا أمة ميئوس منها تتجمع عند الطبول والمزمار ومباريات كرة القدم ، و تفترق مع أول صافرة لحكم مباراة أو دولة أو جهاز أمني سيء !!

التغيير يجب أن يبدأ من الجميع دفعة واحدة ، وعليه يجب أن يعمل في تحقيق هذا الحلم الكبير جميع العلماء المحليين والدوليين ، وأن يتم إرسال نشرات دورية وأبحاث عملية ورسائل حكومية للعلماء والمهندسين في الخارج بهدف جذب العقول ، وتوحيد الجهود والتوجهات في إقامة أمة ذات قوة علمية وثقافية جبارة ، تستأصل أخطاء الماضي وتبني جيلاً يستحق الاحترام والتطور .

تنقسم البرامج المتوفرة على الإنترنت إلى أكثر من قسم ::

Open Source البرامج مفتوحة المصدر

برامج في قمة الروعة ، تم إنشاءها بواسطة أكثر من جهة ، قد يكون طالب وقد يكون عالم ، وقد يكون مجرد هاوي للغة برمجية معينة ، يتم التطوير فيها من الجميع ، ويستطيع الجميع إضافة وتعديل الاكواد البرمجية الخاصة بالبرنامج ومن أمثلتها المشهورة ما قد تراه في الموقع العالمي لهذه البرامج المميزة .

/http://sourceforge.net

وهو موقع يحتوي المشاريع ، ويهيئ لكل مشروع صفحة خاصة للبرنامج ، مع إمكانية تحميل الكود المصدري والتعديل عليه من فريق البرنامج أو غيرهم .

FreeWare البرامج الحرة

وهي برامج يتم تصميمها ونشرها مجاناً (غالباً) ، ويمكنك تحميلها من مواقع البرامج العالمية كالتي تم ذكرها في الفصول السابقة ، ويتم بموجب ذلك إمكانية توزيع وتشغيل البرنامج الحر على أكثر من جهاز .

حقيقة غريبة :: تم إنشاء العديد من جمعيات البرامج الحرة في أوروبا وأمريكا والهند وغيرها ، ولم يتم حتى الآن في الدول العربية .!!!

ShareWare البرامج المشاركة أو المساهمة

وهي برامج ترتكز في الأساس على برنامج أكبر ، بمعنى أنه قد تتثبت بعض البرامج وتجد أنها مجانية في حدود معينة ، كإلغاء بعض القوائم الخاصة بالبرنامج ، أو بعض الإمكانيات وتبرمج الشركات هذه البرامج بغية الإعلان عن المنتج الذي يتم شراءه من المستهلكين فيما بعد .

Trail , Demo Wares برامج كالسابقة تقريبا

مثلا تثبت برنامج فوتوشوب فيطلب منك شراؤه خلال ٣٠ يوم ، وبعد انتهائها لن تستطيع من تصفح البرنامج أو العمل عليه .

Beta برامج في مرحلة التجربة والتطوير

وهي برامج غالبا ما تسبق النسخة الكاملة والمطورة والثابتة من البرنامج ، كأول ظهور لنظام تشغيل سيفين مثلا نزلت نسخة منه Beta ثم طورت الشركة النظام وأصلحت بعضاً من عيوبه بعد آراء المستخدمين والمهندسين وغير ذلك .

ما يهمنا مما تم ذكره التأكيد على أننا ننتصح المستخدم العادي بالتالي :

أولا تثبيت النظام لمدة ٣٠ يوم فقط ، ومن ثم إعادة تثبيت نظام جديد ببرامج جديدة ، ونظرا للسرعة الهائلة في عصر الانترنت اليوم ، تستطيع تحميل معظم البرامج من مواقعها الرسمية في وقت قليل جداً ، وهذا يسمح لك استخدام جميع البرامج دون الحاجة لرقم تسلسلي لأن أغلب البرامج تعطيك برامجها للتجربة ٣٠ يوماً ، وهذا سيوفر لك عدم الحاجة في البحث عن كراك أو أرقام تسلسلية هي في الغالب يتم دمجها بأكواد خطيرة قد تلحق الضرر بجهازك .

بالإضافة أني وفي آخر الكتاب سأتطرق لطريقة سهلة وسريعة في تثبيت النظام .

برامج الحماية من الفيروسات :

أشهر هذه البرامج البرنامج الألماني

[*Avira* AntiVir *Personal* - Free Antivirus]



وهي النسخة المجانية من البرنامج المميز لشركة عملاقة في مجال الحماية ، هذه الشركة والتي تطورت سريعاً واستطاعت اكتساب احترام كثير من المستهلكين والشركات العالمية في مجال أمن المعلومات قدمت نسخة مجانية بالكامل للمستخدم العادي ، سنعتمد على الأفيرا لعدة أسباب مهمة ::

١ – السرعة الرائعة، وعدم التأثير على سرعة الجهاز .

٢ – الأمن العالي إذ يعتبر أصعب برنامج في التشفير الذي يستخدمه الهاكرز.

٣ – قاعدة بيانات هائلة يتم تحديثها يومياً .

٤ – في الفترة الأخيرة بدأت الشركة بالعمل بمبدأ الشر يعم والخير يخص ، وقامت بمقارنة بين طرق الهاكرز والمبرمجين ، وعليه قامت الشركة بمنع البرامج التي يتم صنعها بواسطة الهاكرز أكثر من صنعها بواسطة المبرمجين العاديين سيتم شرحها لاحقاً في دروس الدمج والتلغيم :)

٥ – الشركة ألمانية وهذا تشجيع مني للصناعات الألمانية والدور الذي قد يلعبه من تتلمذ هناك من جاليات عربية ومفكرين وأطباء ومهندسين وغير ذلك (أحلام) .

يتم تنزيل البرنامج من موقعه الرسمي ، وبعدها يتم تثبيته كأي برنامج آخر ، وفور الانتهاء يباشر عمله على الفور .

عند ظهور فيروس معين تخرج شاشة صغيرة تخبرك باكتشاف فيروس نستعرضها معاً في الصورة التالية .



البرنامج سهل جدا في التعامل ، ويقول الكثير من الخبراء الآن بأنه أفضل البرامج في الحماية من الفيروسات ، وارتفعت أسهم هذا البرنامج العملاق بعد عصيه على الهاكرز في تخطيه أو التشفير عنه مع أن أغلب البرامج الأخرى يتم تخطيها من الهاكرز بكل سهولة ، وعليه ننصح المستخدم بتجربة البرنامج ، ولا نفرض عليه شيء ، فقد يستحسن البعض أي برنامج آخر ، وكلها تصب في نفس الزاوية ولها مميزات كما فيها عيوب ومن الصعب جدا أن تعتمد الآن على برنامج مكافحة فيروسات واحد .

وفور انتهائنا من هذا الدرس سنستعرض برامج أخرى لمساعدة برنامج مكافحة الفيروسات بهدف بناء عدة طبقات للحماية ، فإن استطاع الهاكرز الذي يحاول اختراقك تخطي طبقة لن يستطيع تخطي الأخرى ، وسيتم توضيح ذلك بالصورة التالية :



كما ترون رسمنا بشكل مبسط مالذي سيحدث لو حاول أحد الهاكرز اقتحام جهاز ، والعملية بالشرح البسيط ستكون كـالتالي بناءا على ما سيحدث من الهاكرز ::

حاول تشفير فيروس خاص به ، وإرساله إليـك بأي أسلوب أو طريقة يستحدثها هو أيضا في اقتناص ضحاياه .

بذلك قد يتخطى مكافح الفيروس الخاص بك ، وإذا لم تكن لديك الطبقات الأخرى فسيكون من السهل جداً بعدها التجسس عليك بأي أسلوب .

إذا كان لديك جدار حماية جيد ، سيظهر لك رسالة تفيد بأن هناك برنامج يحاول الاتصال بالانترنت ، وإذا تجاوز الجدار الناري أو أخطأت بالسماح له سيحدث التالي .

ستخرج برامج المراقبة الخاصة بك ، وتخبرك بأن هناك برنامج قد أحدث تغييرات معينة ، ويتصل بجهاز آخر وحينها الخيار خيارك في استمرار السماح أو المنع .

إن لم تكن تراقب هذه الاتصالات ، ستخرج رسالة من برنامج منع التجسس ، تخبرك أن هناك برنامج يحاول التجسس عليك ، وتستطيع هنا بخيارين السماح أو المنع بالطبع ..

إن تخطى كل هذه الطبقات وحاول سرقة كلمات المرور ستكون مشفرة بواسطة برنامج سيتم شرحه لاحقا .

إن تخطي كل هذه الطبقات أمر يكاد مستحيلاً لكل الهاكرز وليس الضعفاء منهم ، فهذه الطبقات ستعمل على حماية متكاملة لنظامك ، ليس هذا فحسب وإنما ستحافظ على الدوام على أمان جهازك بشكل كامل حتى لو تم استحداث المزيد من الثغرات البرمجية وتطور أسلوب الهاكرز في الاختراق .

الأهم أن لا تحمل أي ملف من مصدر غير موثوق فيه ، ولا تتصفح الانترنت إلا بعد تطبيق الأمنيات التي تم دراستها في الفصل الخاص بالتصفح ، أضمن لك بعد ذلك أنك لن يتم اختراقك إلا بأمـر منك ، أو سيكون الهاكرز شخصا من ضمن الأشخاص الذي يجلسون على نفس الجهاز الشخصي الخاص بك :)

إلى الدرس الثاني ، وإلى الأمـام في إنترنت خالي من الفيروسات الحاسوبية والعقلية ، التي اجتاحت الكثيـــر ..

الدرس الثاني : برامج الجدران النارية

بعد تبسيط المعلومات قدر الإمكان ، أستطيع أن أخبر المستخدم العادي بأن الجدار الناري هو سد منيع يمكن من خلاله فتح بعض البوابات لمرور بعض المعلومات ، ولا يمكن هذا إلا بإرادة المدير العام للجهاز الشخصي ، فعملية السماح أو المنع فعليا تتركز حول إعطاء المستخدم معلومات عن البرامج التي تحاول إرسال أو استقبال المعلومات بأي هدف كان ، حتى ولو كانت برامج موثوقة ، فلن يتم العبور الفعلي للمعلومات دون موافقة المستخدم للجهاز ، والذي حينها سيكون قادرا على معرفة ما يريد سماحه وما يريد منعه بالتحديد .

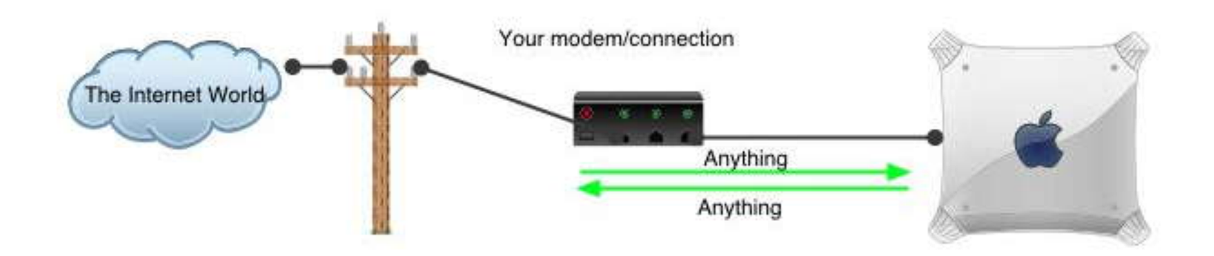


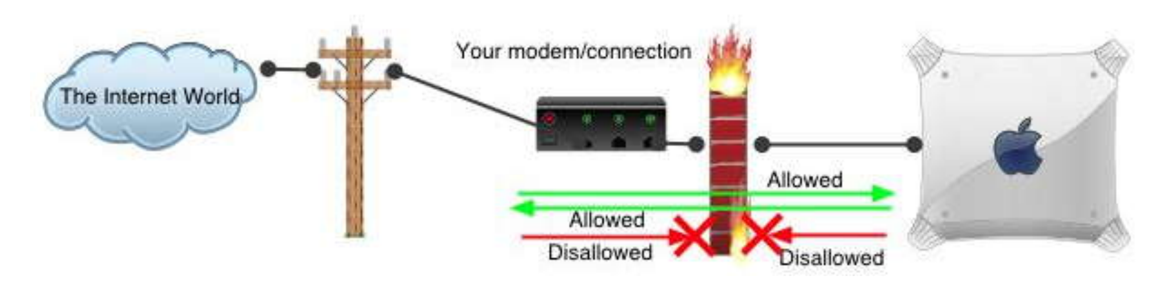
فلو فجأة ظهر لك إحدى البرامج الذي يحاول الاتصال بالانترنت وأنت متيقن بأنك فقط ضغطت على فيديو أو صورة أو أي شيء آخر ، تأكد من أن هناك ما يريب .

سنشرح كيفية التدقيق في هذه الرسالة والكشف على البرنامج المطالب بإرسال أو استقبال معلومات من الانترنت .

بالتالي سنمنع أي هاكرز من الاتصال بجهازنا بأي طريقة كانت ، إلا بعد موافقتنا فيجب علينا التدقيق والحذر في الرسائل التي قد تظهر من الجدار الناري على وجه الخصوص .

وحتى نفهم جيداً العملية هذا الشكل يوضح ما سيحدث بعد تثبيت الجدار الناري





الحالة الأولى بدون فايرول ، الحالة الثانية مع فايرول .

الجدير ذكره أن الجدران النارية تتطور باستمرار ، وذلك رداً على تطور الهاكرز ومحاولاتهم في تخطيها أو تعطيلها قبل عملية الاتصال بالهاكر ، ولكن الكثير منها متشابه كثيرا حيث سنستخدم جدار ناري من ضمن الكثير من الجدران النارية المتنافسة اليوم على ساحة المنتجات ، وطبعا ليس في الساحة البرمجية العالمية منتجاً عربيا ولو واحداً ينافس المنتجات العالمية إلا في مجالات المحاسبة الخاصة بالشركات والأرباح !!

المصنف على أنه الأفضل عالمياً ، برنامج فايرول كان لشركة أمريكية تم بيعها بالكامل لشركة إسرائيلية ومازال الكثير من العرب يستخدمونه ويشترون إصدارات هو وغيره من المنتجات التي تدعم الكيان الصهيوني ،

اسمه Zone Alarm PRO Firewall

ولكن سنستخدم فايرول آخر هو **FortKnox Personal Firewall**

يتم تطويره باستمرار من قبل الشركة المنتجة ، ولا يهمنا تقييم شركات الانترنت العالمية فقد تحابي بعض الشركاء ، ولكن من خلال تجارب وخبرات بسيطة أستطيع أن أقول أنه جيد نسبيا لما يطرح في السوق .

تستطيع الاعتماد على أي فايرول آخر ، ولكن ما يهمنا هنا هو الفكرة في وجوب حصولك على جدار ناري ويعتبر الطبقة الثانية من طبقات الحماية كما أشرنا سابقاً

برنامج FortKnox

سهل جدا كما ستتابع معنا ، ويتشابه مع الجدران النارية في جميع نقاط الشرح التي تهمنا والتي سأذكرها بإذن الله من خلال الصور والإيضاحات التالية :

بعد تثبيت البرنامج ، وإعادة التشغيل نطبق الخطوة رقم 1 للذهاب لقائمة Buy

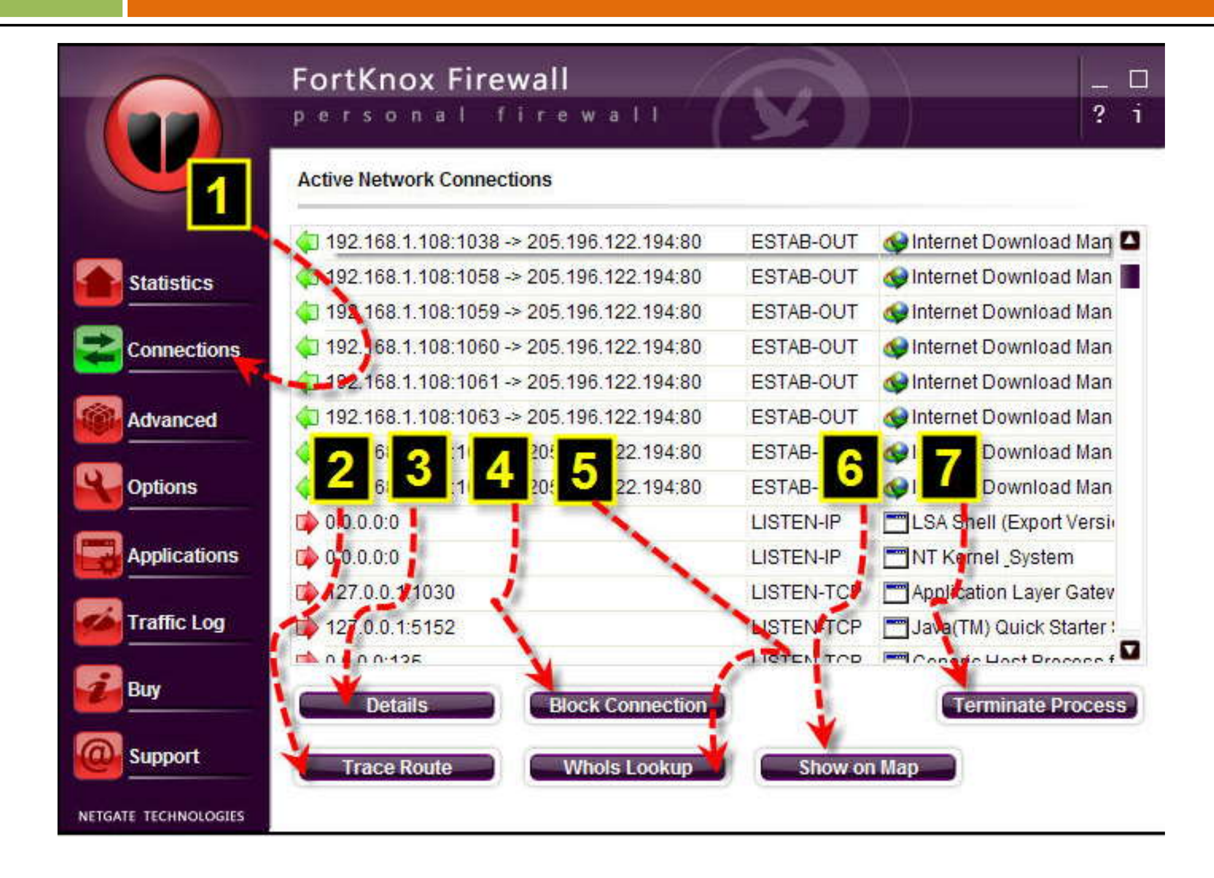
الخطوة 2 لإدخال الرقم التسلسلي الذي سيتم إرفاقه مع البرنامج .



طبعا بهذا نكون قد اشترينا النسخة :)

المهم أننا سنستخدم طرق إدخال السيريالات واللي معه فلوس ما يشتري البرنامج يعمل شركات برمجيات عربية ويوزع برامج الحماية بالذات مجاناً للمستهلكين العرب .

نكمل سوياً ::

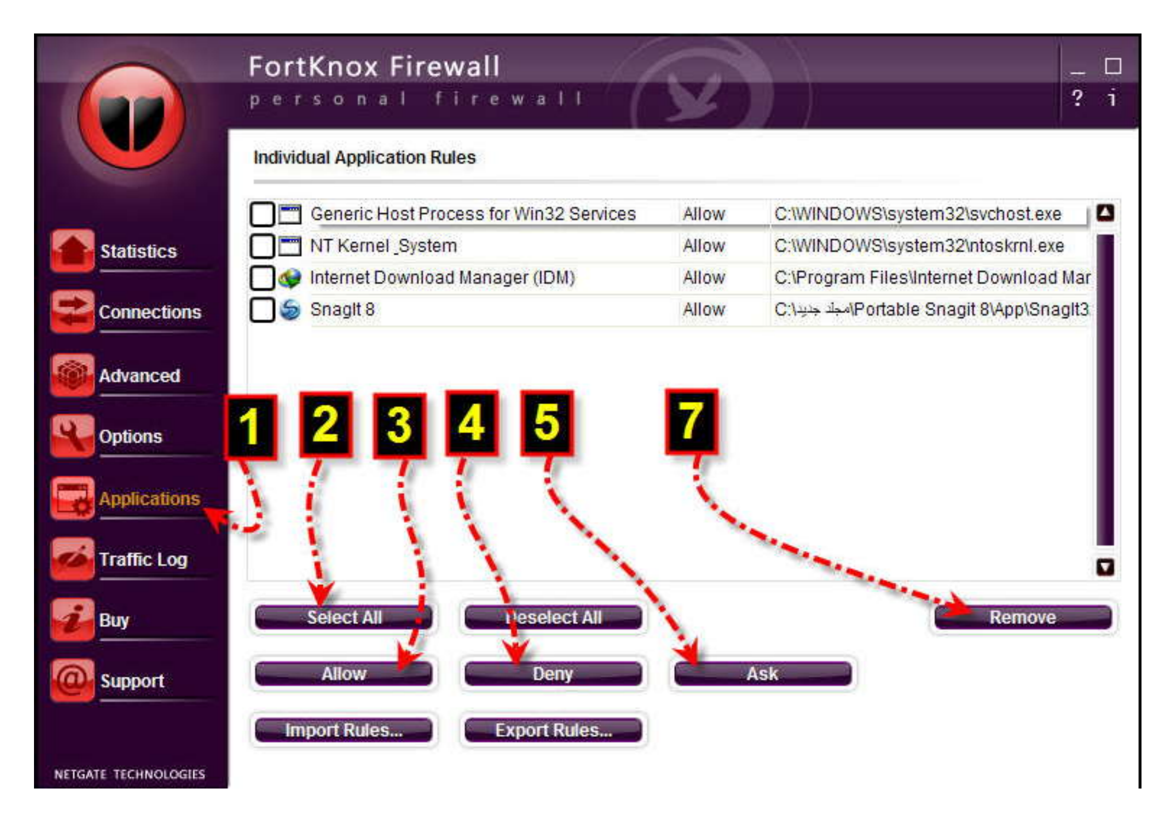


الصورة توضح أننا سننتقل إلى قائمة Connections

لنرى ونتحكم في الاتصالات ، فما نريده يستمر بالعمل ، ومالا نريد فوراً نقوم بحظره كما الحال في الماسنجر بالضبط . :)

دعونا نشرح الأرقام واحداً تلو آخر ::

١ - Connections قائمة الاتصالات
٢ – Trace Route وتعني تعقب السيرفرات (غير مهمة)
٣ – Details تفاصيل عن الاتصال .
٤ – Block Con. حظر الاتصال .
٥ – Whose lookup معلومات أكثر عن الجهة التي يتم الاتصال بها
٦ – Show on map أظهره على الخريطة .
٧ – Terminate Process قتل العملية التي تستخدم هذا الاتصال .



قائمة Applications

وهي قائمة البرامج المسموح لها ، أو التي تم منعها .

وتحتوي على تعديل لقالب القواعد التي تم إنشاؤها ، فلو منعت برنامج عن طريق الخطأ تستطيع إعادة السماح له من خلال الأوامر التالية :

١) Applications قائمة قواعد اتصالات البرامج .
٢) Select All تحديد كل البرامج .
٣) Allow اسمح لهذا البرنامج المحدد .
٤) Deny احظر الاتصال عن هذا البرنامج .
٥) Ask اسألني عندما يقوم بالاتصال .
٦) هو رقم ٧ مش عارف ليه قفزت عنه هههههه
٧) Remove وهو حذف هذه القاعدة .



عند محاولة الاتصال عن طريق أي برنامج ، سيتم إظهار هذه الرسالة ، وهي لب الموضوع كله ، يجب أن تنتبه إلى اسم البرنامج ، وهل فعلا أنت من شغله أعطيت الإذن بتشغيله ، فهذا هو السؤال الهام والذي يجب أن ترد عليه بعد تحديد دقيق ، لماذا تتم عملية الاتصال هذه ، وهل أنا من أعطى الأمر ببدء تشغيلها .

إن كان أنت فتستطيع الاستمرار ، والضغط على yes

ولكن وإن كنت غير متأكد تحاول البحث والتدقيق ، اضغط لا وحاول إعادة فحص قائمة البرامج التي تعمل الآن ، وتتبع معنا كيفية تطوير معرفتك بحركة الفيروسات

والآن شرح القائمة :

١) اسم البرنامج الذي يحاول الاتصال .
٢) الآي بي الذي يحاول البرنامج الاتصال به ، وطبعا هو آي بي موقع في هذه الحالة الخاصة طبعا لأن فايرفوكس كما ذكرنا برنامج تصفح مواقع .
٣) تفاصيل الاتصال ، الآي بي والمنفذ مع سبب الاتصال وهل وارد أم صادر
٤) النصيحة التي يقدمها البرنامج للمستخدم في بعض الحالات .
٥) وهي خانة تخبرك بإضافة قاعدة تسمح أو تمنع بشكل متكرر لاتصالات هذا البرنامج ، فإذا اخترتها وضغط Yes فسيتم اتصال البرنامج بالانترنت دون

عرض قائمة تخبرك بأنه يحاول الاتصال فهل تسمح أو لا ، لأنه سيتم وضع البرنامج في قائمة البرامج الموثوقة ، وإذا ضغط No فسيحدث العكس .
وتستطيع إذا أخطأت ، الذهاب إلى قائمة Applications لتصحيح ومراجعة البرامج المحظورة والمسموح لها .

تستطيع أيضا الذهاب لقائمة Options في أي برنامج جدار ناري ووضع كلمة مرور للبرنامج ، وحينها لن يستطيع أحد تشغيل تلك البرامج إلا بإذن ممن لديه كلمة مرور البرنامج ، وطبعا لن يستطيع إغلاقه .

وبهذا نكون قد شرحنا طبقة هامة من طبقات الحماية ، ونصيحة أن تتابع ما قد يطرأ على مجال جميع البرامج التي يتم طرحها ، فمنها ما يتقدم ويتطور باستمرار تبعا لتطور أساليب الهاكرز ، لذا استخدم هذا الجدار الناري ، أو تستطيع استخدام جدار ناري رائع آخر ، وهو معرب ومن عائلة برامج متنوعة تسمى الشركة Ashampoo وهي من أشهر شركات البرامج العالمية اليوم .

اسمه Ashampoo Firewall

وهو سهل جدا في التعامل ، حاله حال البرنامج الذي تم شرحه .

وأيضا هناك فايرول رائع آخر لشركة عالمية تنمو بشكل سريع في مجال الحماية وهي أول شركة تقدم برامج الحماية بشكل مجاني وبهذا الإتقان الرائع ، فدائما ما يتم طرح البرامج المجانية وتكون مفتقرة لبعض الأشياء التي تتواجد في الإصدار الذي تقدمه الشركة للبيع .

وهي شركة Comodo تستطيع كتابة هذه الكلمة في قوقل وتصفح برامجها ، وسنشرح لاحقاً بعضا من هذه البرامج الجيدة ..

موفقين بإذن المولى عز وجل .

دعائنا لجميع الإنسانية بأوضاع أفضل في ظل تطورات متلاحقة تستخدم العقل تارة ، والعضلات ألف تارة .

ولا حول ولا قوة إلا بالله العلي العظيم .

الدرس الثالث : برامج متخصصة في إزالة التروجان

كما هو الحال في برامج مكافحة الفيروسات إلا أن هذه الطبقة وعلى أهميتها تعتبر من الكماليات ، ولكن تستطيع تضخيم حائط الصد باحتواء جهازك على إحدى هذه البرامج لتضمن تحديداً مختلفاً لقواعد بيانات الفيروسات ، بمعنى أن هذه البرامج متخصصة في التروجان فقط ، وهو البرنامج الضار الذي يرسل لك على هيئة ملف مهم ، بهدف تشغيله من قبلك وعن رضا منك ، ومن ثم يساعد الهاكرز بالدخول على جهازك بكل بساطة ، لأنه خدعك في أي منتدى أو موقع بأن هذا البرنامج هو ما تبحث عنه ، أو حتى أي فيديو وغيره .

لأنه وكما ذكرنا قد يتم تلغيم جميع الامتدادات ، ونكرر الوقاية خير من العلاج .

تعتبر أهميتها في محاولة البحث عن نشاط غير اعتيادي داخل جهازك ، وتتشابه التروجانات في كثير من المواصفات التي تجعل اكتشافها في بعض الحالات سهلا ، أما إن تم صنعها بواسطة خبير برمجي ، فتنبه لأن بعضهم قد يستهدفك بواسطة الهندسة الاجتماعية والتي نحن العرب لا نطبقها في الغالب إلا على أقرب المقربين والأصدقاء والأحباب ، وأغلب من يستخدم الإنترنت يستخدمه بطبيعة طيبة وصادقة وهذا يعتبر نقطة ضعف قوية أصبح يستخدمها الهاكرز في تخطي حوائط الصد التي تبنيها من حولك ..!!

برنامجنا الآن جيد ، وله ماله من مميزات كثيرة سنحاول شرحها من خلال الصور التالية ، والتي تشرح كيفية العمل مع البرنامج ، وتتشابه أيضا هذه البرامج في نفس الفكرة .

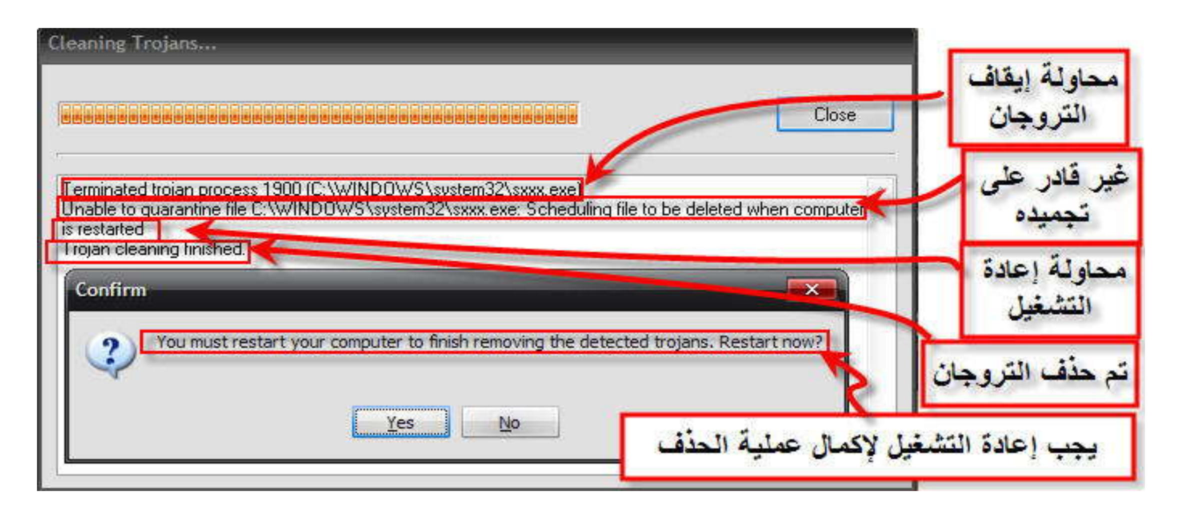
البرنامج الذي سيتم شرحه هو : Trojan Hunter

وهو برنامج مميز جداً تستطيع تحميله من موقعه الرسمي ، ويعطيك فترة تجريبية لمدة ٣٠ يوم تكفينا ، وتستطيع حين الإمساك بأحد التروجانات حذفها إلا أنك لن تستطيع حذف التروجانات في البحث داخل جهازك إلا إذا امتلكت النسخة الكاملة .

بعد تثبيت البرنامج بشكل اعتيادي تابع إذا ما تم التقاط تروجان مالذي سيحدث ::



طبعا هذا التروجان تم تشغيله الآن في جهازك ، وتخطى جميع حوائط الصد التي أسستها سابقاً ، ولكن البرنامج هنا اكتشف التروجان وأظهر لك رساله تحتوي نوع التروجان مع إمكانية الحذف بالضغط على زر **Clean** ، بعد الضغط عليه في معظم الحالات سيتم الحذف بدون ظهور رسالة توجب إعادة التشغيل ، ولكن في بعض الحالات قد تظهر لتأكيد عملية الحذف بالشكل التالي :



كما نرى من خلال الصورة السابقة تمت محاولة الحذف ولكن لم تكمل العملية إلا بعد إعادة تشغيل الجهاز ، يجب تشغيل الجهاز بشكل فوري حين ظهور هذه الرسالة حتى لا يتمكن الهاكر الذي اخترقك من التعامل مع هذا البرنامج وتعطيله .

إلى هنا نصل إلى نهاية هذا الدرس ، تابعونا للمزيـد وفقكم الله .

هناك برامج كثيرة متخصصة في التروجان ولكنها جميعا تتشابه في الآلية السابقة.

الدرس الرابع : برامج مكافحات التجسس المتطورة

Zemana AntiLogger

حصل البرنامج على العديد من الجوائز العالمية ، ومازال يحصد المزيد منها وذلك لمميزاته الجبارة ، وسهولة استخدامه هذا بالإضافة إلى أنه يدعم عدد كبير من اللغات من بينها العربية .

مميزات البرنامج :

يستطيع تحذيرك عند قيام أحد البرامج بالتالي :

محاولة التجسس على ضربات الكي بورد .

محاولة التجسس على المايكروفون .

محاولة التجسس على الكاميرا .

محاولة زرع قيم داخل عقل النظام .

محاولة التجسس على سطح المكتب بالتقاط صورة له .

محاولة زرع أو تعديل قيم في عقل النظام .

يعتبر هذا البرنامج أهم برنامج للمستخدم العادي ، ويراقب جميع الجهاز بأسلوب غاية في الإتقان والروعة ، ومؤخراً فشل الكثير في تخطي هذا المارد الذي سيزيد الحصن قوة وفعالية .

شرح البرنامج :: بعد تثبيت البرنامج نقوم بإعادة التشغيل ، ومن ثم إغلاق البرنامج من جوار الساعة ، وبعدها نشغل الكيجن المرفق مع البرنامج كما في الصورة التالية :

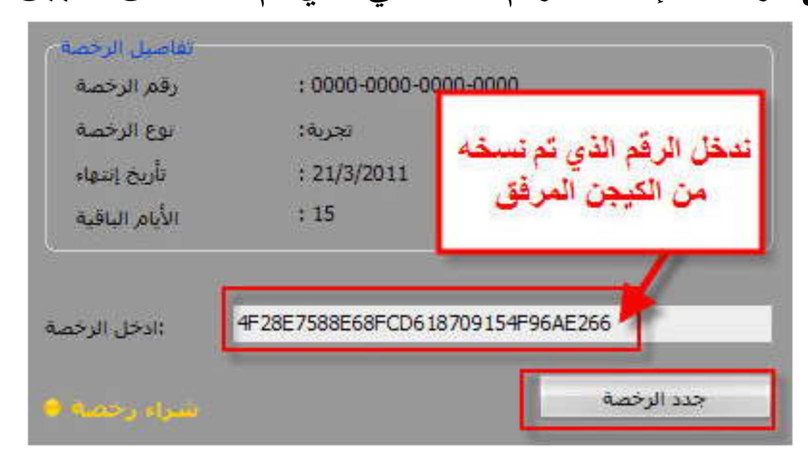


ملاحظة هامة : لا تقم بعمل هذه الخطوة قبل التأكد من وجود جدار ناري يمنع اتصال البرنامج بموقعه لتثبيت التحديثات الخاصة به ، حيث أن هذه العملية ستلغي التسجيل وإذا ظهرت رسالة لتحديث البرنامج اضغط لا .

نشغل البرنامج ونذهب لقائمة الخدمات ، ومن ثم الرخصة كما نرى في الصورة التالية ::



نضغط على الرخصة لإدخال الرقم التسلسلي الذي تم نسخه من الكيجن



كما ترون ، ومن ثم نضغط على زر (جدد الرخصة) .



بهذا نكون انتهينا من تثبيت وإعداد هذا الحصن الجديد ، والذي سيظهر أي خلل قد يطرأ على الجهاز ، فلو حاول برنامج تثبيت نفسه داخل النظام أو تعديله أو التجسس مثلما ذكرنا في المميزات ستظهر رسالة تفيدك بوقوع ذلك ، وتخيرك ما بين السماح وعدم السماح ، كما سنرى في الصور التالية ، والتي سيتم فيها شرح الرسائل بالتفصيل الممل حتى لا يقع المستخدم في حيرة بين ما يسمح وبين ما يرفض ، أولاً يجب أن نؤكد على أن البرامج وحدها لن تحميك ، يجب أن تفهم جميع ما جاء في هذا الكتاب فهماً جيداً وتطبقه حتى تتمكن من الوصول إلى درجة الحماية الكاملة ، وهذا لأن البرامج قد تعطيك هذه الرسائل حتى للبرامج المفيدة والتي أصلا أنت تقوم باستعمالها لأن عقل البرنامج لا يستطيع التمييز في كل شيء

الرسالة الأولى ::



مثلما ذكر داخل الصورة بالضبط ، فهنا يخبرك بأن البرنامج واسمه 000.exe

يحاول التعديل على عقل النظام واكتساب صلاحية دخول كاملة ، وهذا ما تفعله معظم ملفات التجسس في بداية الأمر ، لتفتح منفذ لمرور الهاكرز والذي سيعطي أوامره بالتجسس على باقي النظام ولكن لن يتأتى ذلك له لو ضغطنا زر قفل .

أما في حالة السماح فسيتم اختراقك ، وبالتالي ستظهر المزيد من القوائم والتي تخبرك بأنشطه معينة يقوم بها الهاكرز ، ويعطيك البرنامج في هذه الحالة فرصة لاكتشاف عملية التجسس ،نقطة مهمة وهي زر عرض تفاصيل أكثر وهو لعرض موقع البرنامج بالضبط ، ويمكننا بعد الضغط على زر قفل الذهاب لموقع الملف وحذفه من هناك في حال تأكدنا منه .

أما النقطة الأخيرة فلاحظ هنا مستوى الخطر ، ودائماً حاول أن تلاحظ كل شيء .

نتابع سلسلة الرسائل التي قد تظهر إذا أراد الهاكرز التجسس عليك بوسائل مختلفة

الرسالة الثانية ::



هذه الرسالة تخبرك بأن البرنامج 000.exe يحاول الاتصال بالميكروفون الخاص بك ليعمل مكالمة صوتية ، وهو ما سيحدث إذا قام الهاكرز بالتجسس على المايك الخاص بك .

الرسالة الثالثة ::

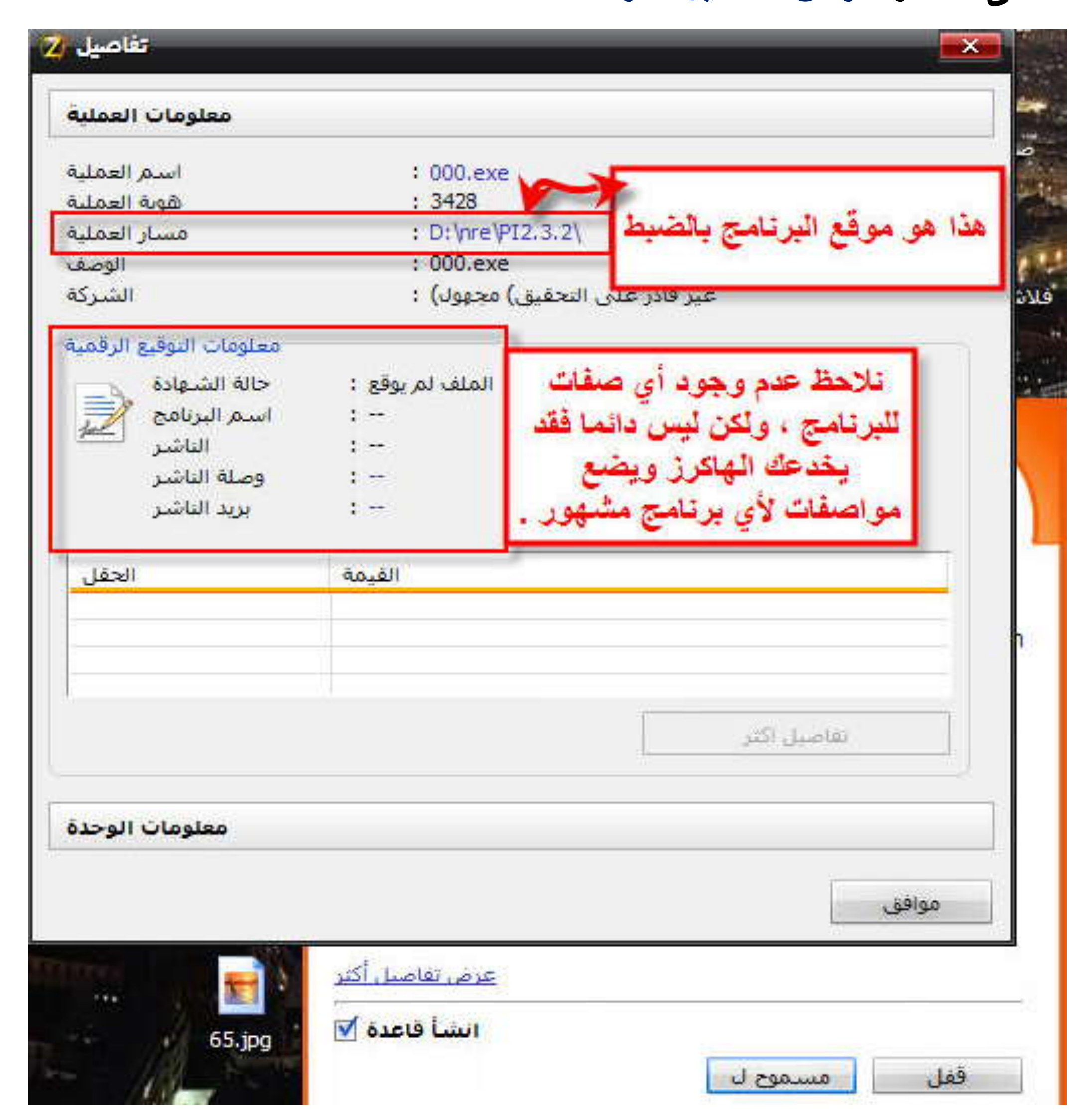


وتعني أن البرنامج 000.exe يحاول التقاط صورة لشاشتك ، إياك أن تضغط السماح قبل معرفة البرنامج طبعا ، وفي كل مرة يحذرك فيها ينصحك بعدم السماح إلا بعد التحقق من البرنامج .

نكتفي بهذا القدر من الرسائل فالباقي يشبه هذا أو يختلف قليلاً ،

المهم أننا كيف سنميز بين الإنذار الحقيقي والكاذب ..؟؟ ،

اضغط على السطر عرض تفاصيل أكثر



تظهر هذه القائمة وما يهمنا منها لقطع الشك باليقين هو مسار البرنامج ، نضغط على السطر فيفتح لنا متصفح الملفات ويختار البرنامج بالضبط ، نرفعه على إحدى مواقع فحص الملفات ونرى ماهيته بالضبط .

وسيتم شرح هذه النقطة بالتفصيل أي رفع الملفات لفحصها على الإنترنت في درس منفصل بالتفصيل إن شاء الله .

الدرس الخامس : برامج تشفير الكتابات والملفات الخاصة

سنقوم بشرح برنامجين ، وطبعا تستطيع استخدام مئات البرامج التي تحمل نفس الهدف ، ففي النهاية يجب أن تحدد ما هي الطبقات التي ستعمل على إنشاؤها لحماية جهازك ، وسواء اخترت البرامج التي تم شرحها أو غيرها ممن يحمل نفس المواصفات تكون قد وفرت هذه الطبقة من الحماية .

وإن شاء المولى عز وجل ستتجاوز أي طفل من أطفال الهاكرز .

البرنامج الأول : KeyScrambler

برنامج متخصص في تشفير ما تكتب بخوارزميات مختلفة ، بمعنى أن التشفير المستخدم يتغير في كل مرة تقوم بالكتابة ، ويستحيل ترجمة النص بأي وسيلة كانت أو عبر أي برنامج لأن البرنامج تختلف خوارزميته في تشفير الكلمات ، فلو فرضنا مثلا أن شخصا ما قام باختراقك ، وراقب ما تكتب من كلمات مرور أو بريد أو أي شيء ، سيظهر له رموز وكلمات مختلفة اختلافا كليا ، ولن يتمكن من الوصول إلى كلمات السر الخاصة بك نهائياً .

شرح البرنامج

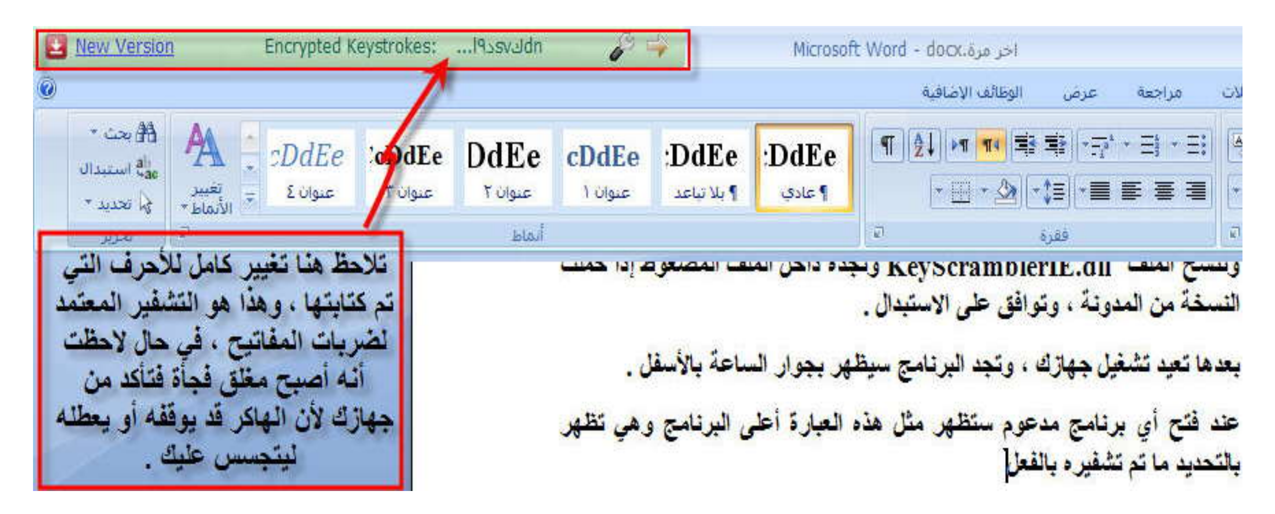
بعد تثبيت النسخة Premium بشكل اعتيادي كأي برنامج آخر ، نذهب إلى الموقع

C:\Program Files\KeyScrambler

وننسخ الملف KeyScramblerIE.dll ونجده داخل الملف المضغوط إذا حملت النسخة من المدونة ، وتوافق على الاستبدال .

بعدها تعيد تشغيل جهازك ، وتجد البرنامج سيظهر بجوار الساعة بالأسفل .

عند فتح أي برنامج مدعوم ستظهر مثل هذه العبارة أعلى البرنامج وهي تظهر بالتحديد ما تم تشفيره بالفعل



طبعا البرنامج يشفر بأسلوب مميز جداً لا يمكن بأي حال من الأحوال فكه ، حتى لو وصل لأيدي هاكرز ، وذلك لأنه يعتمد خوارزميات مختلفة وتتغير باستمرار .

البرنامج الثاني :: True Crypt

يستخدم في إغلاق الملفات بكلمة سر ، وهو تشفير مميز يمنع المخترق من التقاط الملفات المشفرة إطلاقاً ، ويجعل من المستحيل على الهاكرز تعديل الملفات حتى لو استخدم أي تكنولوجيا في ذلك ، ولكن قد يتم فك تشفير الملفات إذا ما حاول تجريب ملايين الاكواد ويحدث ذلك حين تشغيل برنامج ولكن هذا لا يستخدم إلا من خلال أجهزة ضخمة لا تمتلكها إلا أجهزة المخابرات لأن الأجهزة العادية قد تستغرق سنوات في فك الشفرة .

وهنا يجب أن تضمن ما سأقوله لك ، إياك أن تعتقد أن التجسس عليك مستحيلاً وغير ممكناً ، فكثير من الأطراف الدولية تستطيع استخدام التكنولوجيا التي بيديك للوصول إليك وطبعا سيستخدمون الهندسة الاجتماعية (البحث المتواصل على ثغرة في الشخص وتفكيره وليس في الجهاز الخاص به)

إياك أن تستخدم التكنولوجيا في التصوير الخاص !!

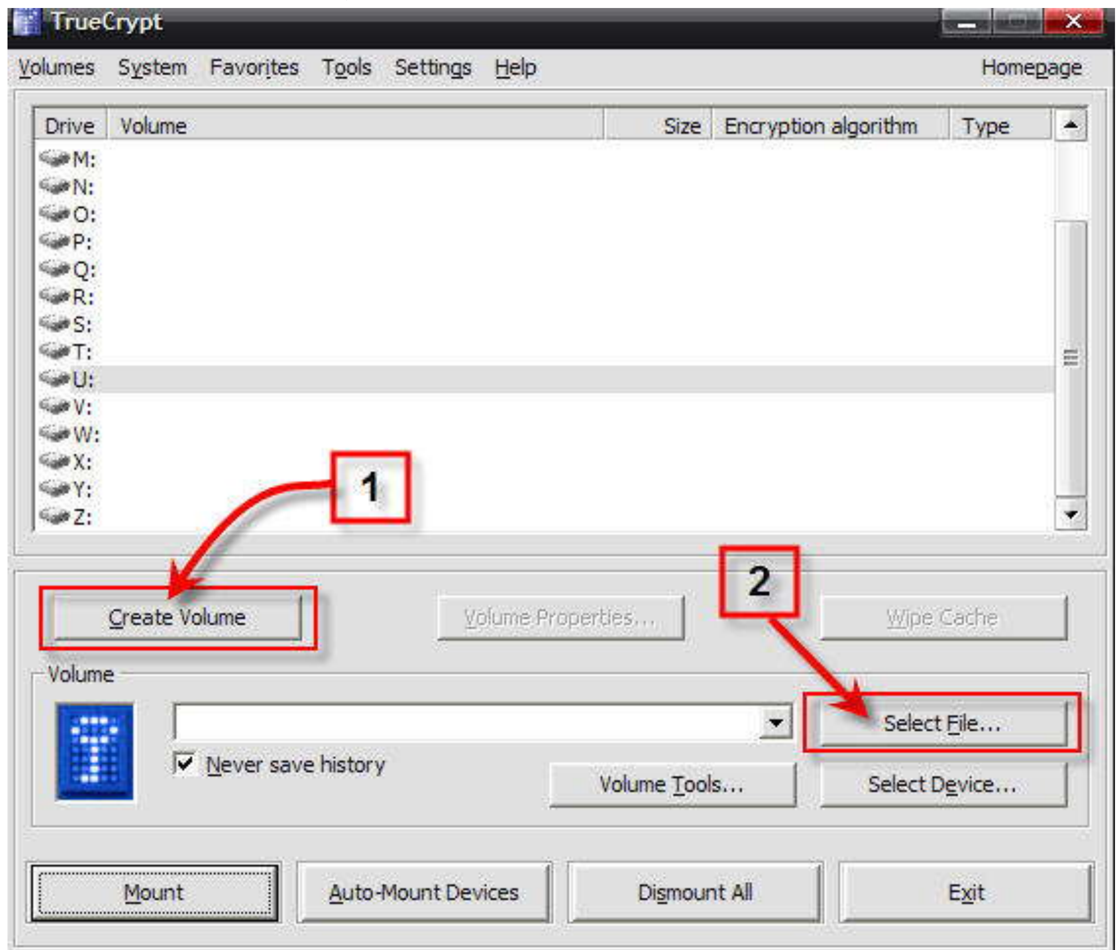
إياك أن تستخدمها في حفظ ذكرياتك وأسرارك !!

إياك أن تحتفظ بما ستره الله !!

إياك أن تنشر شيئاً فيه اعتداء على الآخر ، فقد تصبح يوماً ما ذات الشيء المنشور .. !!

شرح البرنامج ::

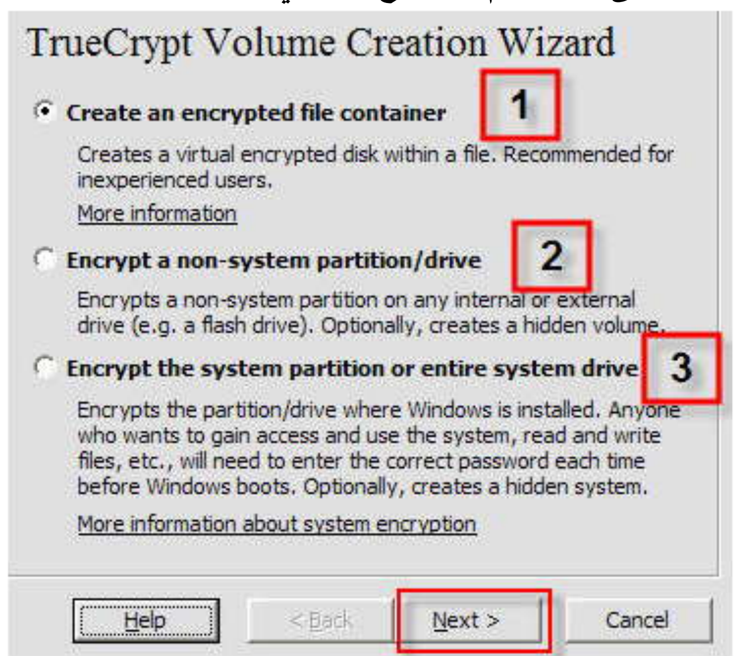
بعد تثبيته نفتح البرنامج وستظهر القائمة الرئيسية كالتالي :



١ – هذا الزر لإنشاء قرص مشفر جديد .

٢ – هذا الزر لاختيار قرص تم إنشاؤه سابقاً .

عند الضغط على الزر رقم ١ نتابع كالتالي ::

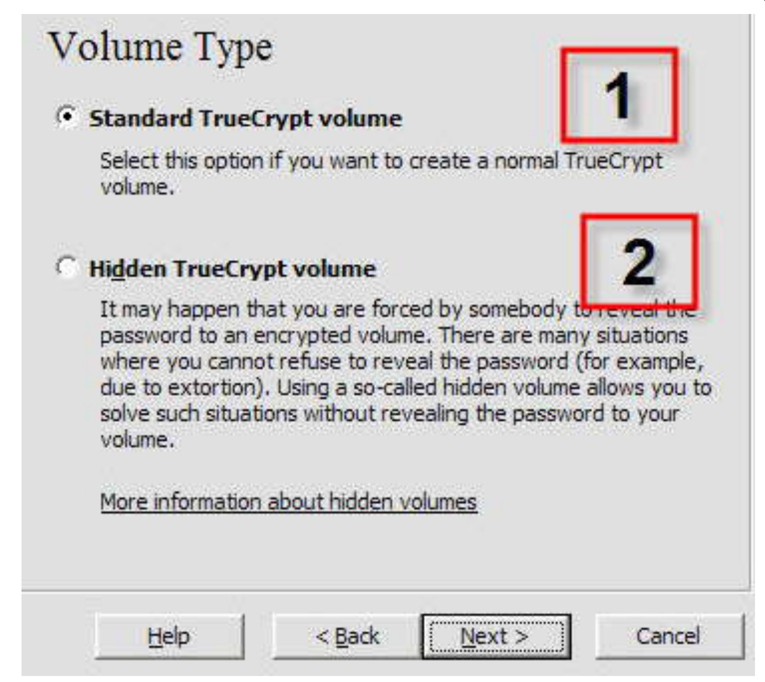


١ – تعني إنشاء قرص جديد مشفر .

٢ – تشفير قرص غير قرص النظام .

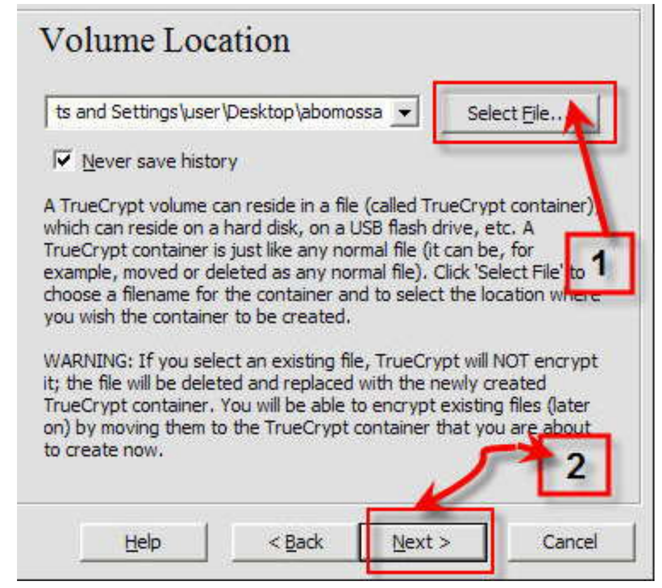
٣ – تشفير قرص النظام .

من الأفضل كـ مستخدم عادي تجربة الخيارين الثاني والثالث على الآلة الوهمية وإتقان البرنامج ومن ثم تطبيقه على الجهاز الحقيقي حتى لا تحدث أي مشاكل معك بإذن الله . نتابع بعد اختيار الخيار الأول ::



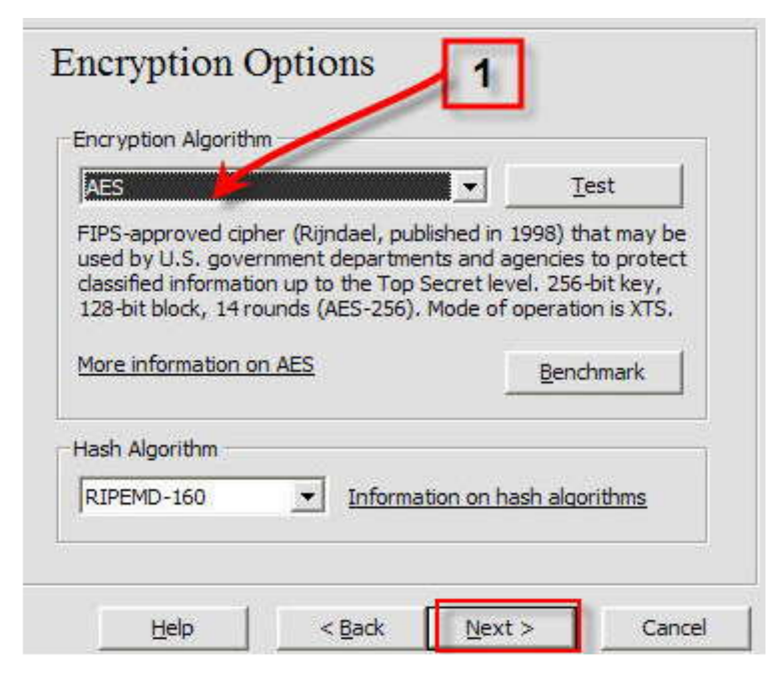
١ – تعني إنشاء قرص عادي بالمواصفات الاعتيادية .

٢ – تعني إنشاء قرص مخفي ، نختار الخيار الأول ونكمل ::



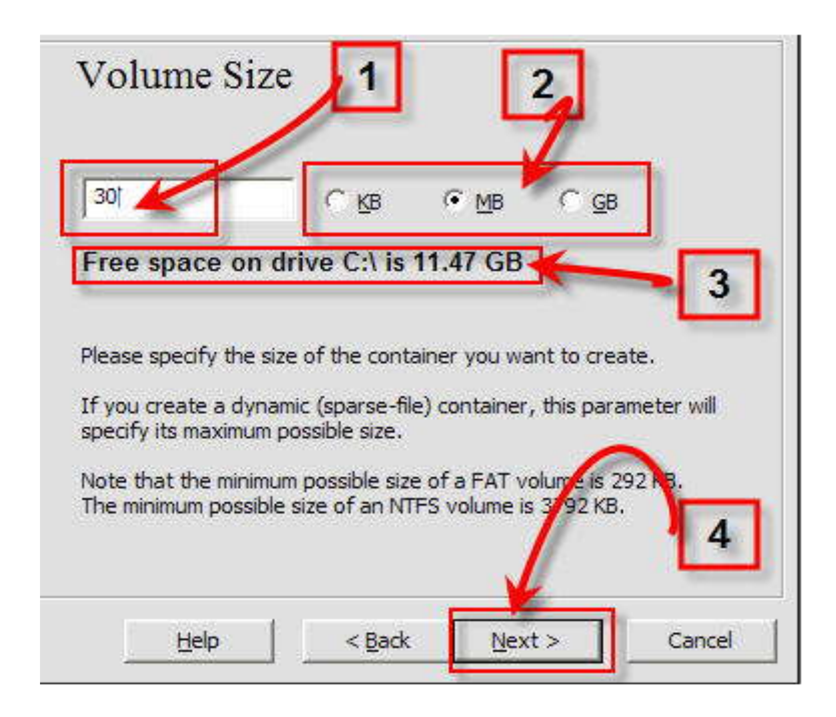
١ – نختار اسم القرص ومكانه بالضبط .

٢ – نختار دائماً زر Next للمتابعة .



١ – نوع التشفير تستطيع الاختيار بين أي من الأنواع في القائمة .

يفضل ترك الإعدادات كما هي فهو تشفير قوي جداً ، ومن المستحيل على هاكرز عادي فك التشفير ببساطة ، نضغط Next ونتابع ::



١ – حجم القرص الذي تريد إنشاؤه .

٢ – نختار الحجم بالكيلو أم الميقا أم القيقا

معلومات بسيطة عن الكيلو ويساوي ١٠٢٤ بايت ، أما الميقا فـ ١٠٢٤ كيلو بايت أما القيقا فيساوي ١٠٢٤ ميقا بايت ، والتيرا يساوي ١٠٢٤ قيقا بايت .

٣ – المساحة الحرة في القرص الذي اخترت أن يكون القرص المنشأ داخله وهي أقصى مساحه تستطيع اختيارها للقرص المشفر .

٤ – اضغط Next أيضـاً .

Volume Password

Password: ***

Confirm: ***

Use keyfiles — Keyfiles...

Display password

It is very important that you choose a good password. You should avoid choosing one that contains only a single word that can be found in a dictionary (or a combination of 2, 3, or 4 such words). It should not contain any names or dates of birth. It should not be easy to guess. A good password is a random combination of upper and lower case letters, numbers, and special characters, such as @ ^ = $ * + etc. We recommend choosing a password consisting of more than 20 characters (the longer, the better). The maximum possible length is 64 characters.

Help | < Back | Next > | Cancel

هنا تختار كلمة السر التي تريدها للقرص الذي يتم إنشاؤه .

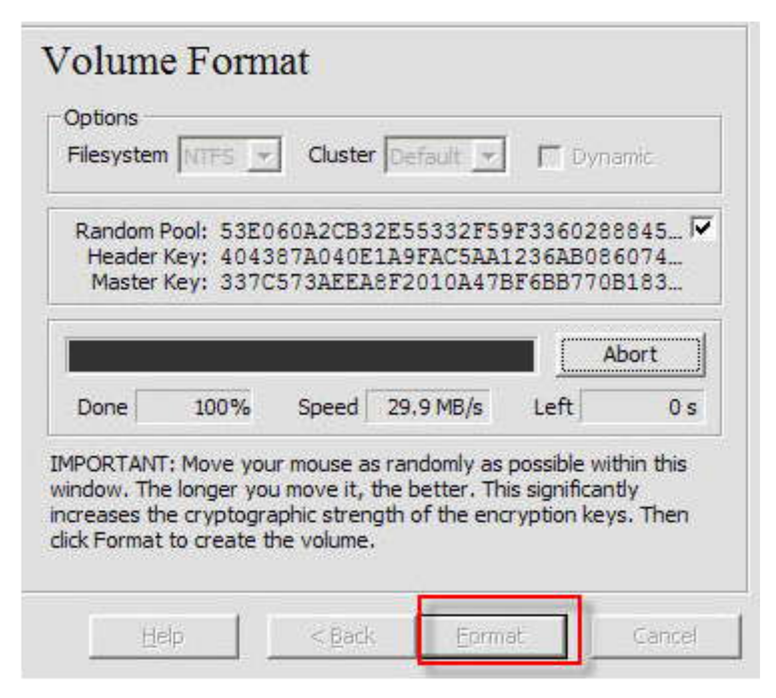
WARNING: Short passwords are easy to crack using brute force techniques!

We recommend choosing a password consisting of more than 20 characters. Are you sure you want to use a short password?

نعم | لا

ستظهر هذه الرسالة لو كانت كلمة السر أقل من ٢٠ حرف ، من المفضل جداً أن تختار كلمة سر ضخمة تحتوي على أكثر من عشرين حرف ورمز ورقم ، ذلك حتى يصعب فك تشفير الملف .

تضغط نعم للاستمرار ،



تظهر هذه القائمة تختار File system يفضل أن تكون من النوع NTFS

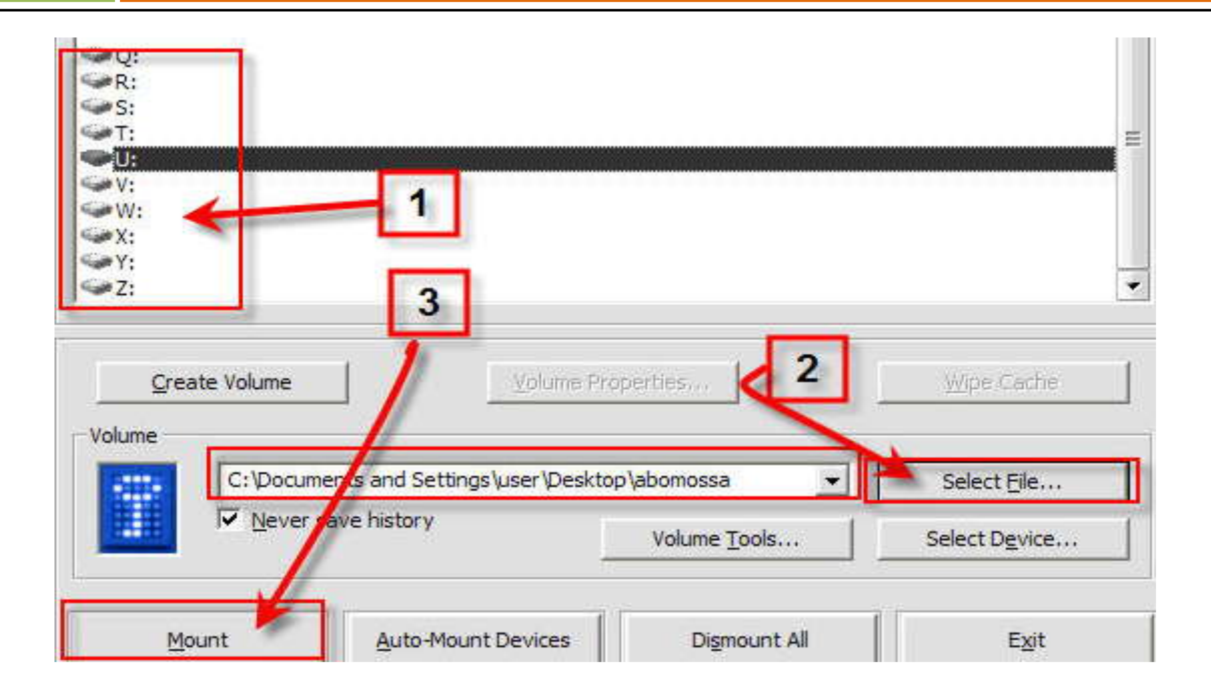
ثم تضغط زر Format



هنا يخبرك بأنه تم إنشاء القرص بالمواصفات وكلمة السر التي اخترتها .

تضغط Exit لو ضغط Next فستعود القائمة من جديد لتنشئ قرص جديد بمواصفات جديدة ، أما لو اكتفيت بهذا القرص تضغط Exit

إذا أردت إضافة ملفاتك ليتم تشفيرها داخل الملف الذي أنشأته تتابع في الواجهة الرئيسية كالتالي ::



١ – اسم القرص الذي سيتم تركيب الملف عليه .

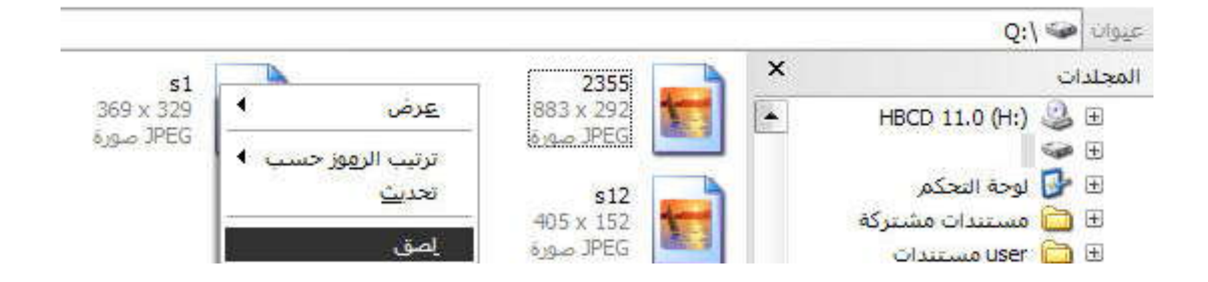
٢ – تختار الملف المشفر الذي تم إنشاؤه في السابق .

٣ – بدء عملية تركيب الملف كقرص لتتم عملية نسخ ملفاتك عليه ومن ثم تشفيرها .

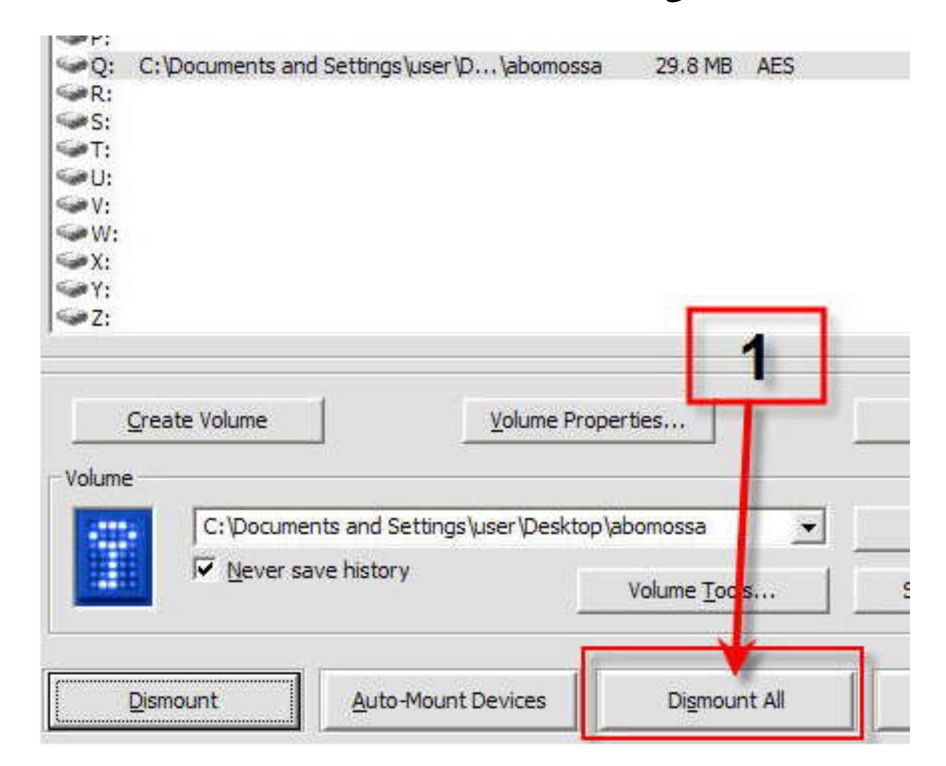


تلاحظ ظهور القرص في قائمة الأقراص الخاصة بك .

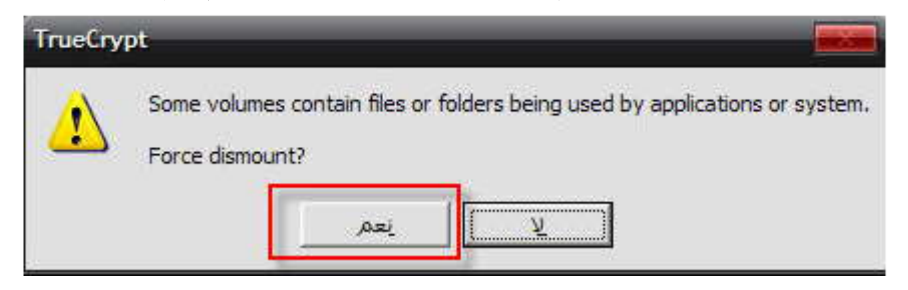
تفتح القرص وتنسخ عليه الملفات التي تريد تشفيرها كالتالي :



بعد الانتهاء من نقل جميع ملفاتك التي تريد تشفيرها من الواجب إزالة القرص مرة أخرى ، بالضغط على زر Dismount All



١ – Dismount All وتعني إزالة جميع الأقراص التي تم تركيبها .



إذا ظهرت لك هذه الرسالة معناها أنه بعض الملفات في القرص المشفر يتم استخدامها ، أضغط نعم لفرض عملية إلغاء التركيب وإغلاق القرص .

تم بحمد الله شرح أفضل برامج التشفير الموجودة حالياً ، وهو برنامج مميز ومجاني بالكامل ، هذا وفضلنا شرحه بالتفصيل ذلك لأننا ننصح وضع جميع الملفات الخاصة في أقراص كالتي سبق طرحها ، ووضعها داخل اسطوانات حتى لا يستطيع الهاكرز حذفها حتى لو اخترق الجهاز المستهدف .

نصائح مهمة : يفضل فصل الانترنت عند عملية تصفح الملفات المشفرة .

دمتم بكل حمايــة وسعادة وخيــر .

الدرس السادس : مراقبة التغيرات في النظام

قبل أن يتم تثبيت أي برنامج جديد مشبوه ، يجب أن يتوفر لدينا الآتي :

١ - نظام تشغيل وهمي .

٢ – يفضل أن يكون بدون إنترنت .

٣ – يتم تثبيت الطبقة السادسة (هذا الدرس) وهي أهم الطبقات حتى تتابع بالتحديد ما هي الملفات المثبتة بالضبط .

٤ – يتم فحص جميع الملفات والتعديلات بواسطة خبرة بسيطة في مجال الكومبيوتر ، وبالنسبة للمستخدم العادي فنرجو أن يتسع صدره لما سنقول ويحاول أن يطور معلوماته قليلا في أحدث طرق الفحص المكتشفة لكشف التلغيم والدمج .

في البداية يجب أن نعلم أن أي نظام في العالم لأي شيء حتى الإنسان والحيوان ، والأنظمة السياسية والاجتماعية والأسرة وغيرها من كل تلك الأمور النظامية تحتاج ظروف معينة لتعمل وتستمر وتتطور .

ونظام التشغيل لديك أيضا لديه نفس هذه الميزات ،

فهو مصمم ليحاكي النظم البشرية في شتى مراحلها ، فهو يحتوي على عقل برمجي منظم ، وملفات معينة تساعد في الإدارة .

إلا أن عقل النظام هو المسئول عن تشغيل أو منع تشغيل أي ملف آخر ، وأي تعديل يطرأ على الكومبيوتر هو من صنع هذا العقل الذي تم تصميمه لإدارة النظام ككل ، وإن حدث تعارض ما في البرامج فسيكون الخلل موجوداً في عقل النظام ، وإن حدث وضرب فيروس ما النظام ، ففي هذه الحالة سيصيب عقل النظام ، وحتى عند إرسال ملف تجسس لنظامك ، فإن أول ما يستهدف هو عقل هذا النظام ، والذي يأمره بفتح بعض البوابات لدخول الهاكرز الحقيقي .

كل هذه الأمور قد تكون صعبة على البعض إلا أني أفضل شرحها بالتفصيل فجميعنا يريد أن يحمي نفسه ، ولن يمل بقراءة بعض الأمور التي ستثير تفكيره الشخصي

في طبيعة الحاسب الآلة الجامدة التي أمامه ، وطبيعة تفكيره في عقله هو الإنسان الحر الذي يفرض تطور أو تخلف نفسه .

عقل النظام يسمى بـ الريجيستري وهو برنامج معين لا يتم بدء النظام دون أخذ الإذن منه ، ويشكل عقل النظام الجزء الوحيد الحساس جداً ، فأي خطأ قد يحدث داخله قد يتسبب بانهيار النظام ، لذا فإن أي فيروس في العالم تم اختراعه كان يستهدف هذا العقل ويحاول استثارته لأغراض أخرى غير التي تم صنعها لأدائها ، فيبدأ هذا العقل بإصدار أوامر غريبة عليه قد تكون عشوائية ، مما ينتج عنه في النهاية وصوله لمرحلة التبلد التام ومن ثم عدم القدرة على الاستمرار وبالتالي انهيار النظام ككل ، وهذا ما يحدث كثيراً لبعض الأنظمة التي قد يطول استخدامها ، أو قد يثبت الشخص كثير من البرامج دفعة واحدة ، فيتفاجأ بأن نظامه لم يعد على قيد الحيـــاة .

كثير منكم قد وصل نظامه أكثر من مرة وعلى مدار فترات معينه إلى مرحلة الانهيار المفاجئ والذي قد يحدث نتيجة أسباب برمجية داخلية ليس لها علاقة بالفيروسات ، أو لها علاقة بالفيروسات ، أو وصول هذا العقل إلى أوامر برمجية كثيرة تسبب شلل تام في استكمال الوظائف المنوطة به فينهـــار ، أو يستمر النظام بالعمل طويلاً دون تغير جوهري فيه لأنه تعود على روتين معين يقوم به في كل مرة نقوم بتشغيله ، ولكن مالذي يحدث عند محاولتنا تغيير هذا الروتين سيسبب هذا تطوراً مفاجئاً قد يتماشى العقل البرمجي معه في إحدى اتجاهين لا ثالث لهما وهما الاتجاه الأول نحو تطبيق هذه التطورات الجديدة والالتزام بها ، أما الاتجاه الثاني فهو يتم فرضه عليه من بعض الإضافات التي قد تعيق عمل النظام ، وتلزمه بالانهيار وعدم الاستجابة .

سنوضح من خلال وصف عقل الحاسب بالعقل البشري :

ما يحدث للعقل البشري في بعض الحالات ، وهي الحالات التي يعيشها أغلب سكان البشرية .

فهم منهارين عقلياً ، ويمارسون حياتهم حسب روتين معين تم برمجتهم عليه لسنوات طويلة من خلال الأسرة وضغط الوالدين والجيران ، والمؤسسات التعليمية هذا بالإضافة إلى الجو العام مع الأصدقاء ناهيك عن دور الحكومة في زرع بعض الأمور البرمجية الداخلية في عقل الفرد ، وكأن الجميع يقول أني مجرد فرد داخل مجتمع واسع وضخم وكبيـر ، فكيف لي أن أغير نفسي والمجتمع كيف لي أن

أصحح مساري ومسار الجميع ، وكيف يتأتى أصلا ذلك وأنا أسير في روتين الخطأ ومن ثم الاستغفار ، الخطأ ومن ثم التوبة .

وعليه كان لا بد ممن يساهم في مراقبة وتعزيز النظام ، فما يصلح يمر ، وما لا يصلح لا يمر ، أما في حال دخول أحد الأشياء عنوة فإذا لم يتم القضاء عليها فوراً فستجلب أخطارا عظيمة تنتهي بانهيار عقل النظام وكافة أجزاءه معه .

وحتى وإن حاول البعض تصحيح الخطأ ، فلن يتم أبداً العودة للوضع الطبيعي ، فهذا مستحيل علمياً وعملياً ، بمعنى يرجع إلى أذهاننا ما كررته مراراً

الوقـاية خير من العلاج .

جميع برامج المراقبة ، تعتبر متشابهة ولكن يكمن الاختلاف في مراقبة نوعية النشاط ، فمنها ما يراقب نشاط قديم فقط ، ومنها ما يراقب الأنشطة التي تطرأ ولا يعنيه ما مر ، ومنها ما يراقب كل شيء سواء قديم أو جديد .

حتى لا يتوه المستخدم العادي سأعمل على شرح برامج بسيطة وغير معقدة إطلاقاً ، وهي مهمة جداً في فحص أي برنامج مشكوك في أمره ، ولكن نعود لنؤكد على أن البرامج الحرة والمفتوحة المصدر منتشرة كثيرا في عالم الانترنت ونفضلها على غيرها ، فالوقاية خير من العلاج .

البرنامج الأول : Autoruns

هذا البرنامج الرائع من إنتاج شركة مايكروسوفت ، حيث عهدت مايكروسوفت لشركات أمنية تطوير بعض البرمجيات ومن ثم يتم دعمها أو شرائها عبر مايكروسوفت ، وحدث هذا لتطوير العقول العالمية التي تسير من أجل دعم الأنظمة التشغيلية ومكافحة الاختراق الإجرامي الذي لا يميز بين أحد وأصبح يستهدف الجميع بلا استثناء حتى أن تكنولوجيات عمليات الاختراق أصبحت في أيدي أطفال الهاكرز الذي يبذرون فيروساتهم على المواقع العالمية بلا أي مسئولية أو رادع إنساني ونفسي ، فأين الضمير المفترض زرعه في الأشخاص وخصوصا العرب نجد أن أكثر هؤلاء المجانين في قمة الراحة المادية ، بالإضافة إلى أنهم متخصصون في التجسس على العرب إخوانهم وكشف عوراتهم وفضحهم ، من خلال تصويرهم أو سحب ملفات تخصهم ، أو أي أسلوب حقير آخر ومن ثم نشر ما حصلوا عليه هذا طبعا بعد محاولة ابتزاز الشاب أو الفتاة المخترق ، وفي الحالتين رفض عملية الابتزاز أو قبولها للأسف يتم نشر ما حصلوا عليه وترويجه داخل

عالم لا يرحم ، ينقل المعلومات بغض النظر عن ماهيتها بسرعة الضوء ، خصوصا لو كانت هذه المعلومة فيديو فضيحة لعربي !!!!

لا حول ولا قوة إلا بالله ، يخبرنا موقع قوقل بأن من أكثر الكلمات التي يتم استعمالها عربيا (فضيحة – فضائح – صور عربية – الخ) من كلمات الرذيلة ، ولكن هذه الكلمات ليست وحدها ، ولكني والله أتفاجأ دوماً بما يحدث معي من قراءة الإحصائيات العالمية ، بعض الأحيان والله أتخبط كثيرا وأغرق في شعور الإحباط من واقعي وواقع الكثير من الإخوة العرب ، فتفاجئني الإحصائيات أن كلمات كـ (القدس – إسلام – فتوى ... الخ) تتكرر كثيراً أيضاً ولو بنسب أقل ، صراحة ليس هناك تناقضاً إطلاقاً فقد تعودنا منذ الصغر على أننا غير معصومين عن الخطأ ، وأننا نستطيع ارتكاب بعض الأخطاء البسيطة لأن الأخطاء تم ترتيبها تنازليا من الشرك بالله إلى أبسط هذه الأخطاء مما أحدث في النفس العربية والإسلامية ميلاً لتجريب الخطأ ومن ثم التوبة ، فحتى من لا يخطئ يستذكر مثل هذه المقولات :

قال (ابن القيم) عليه رحمة الله وكل ابن آدم خطاء وخير الخطاءين التوابون كلنا ذوو خطأ في صحيح [مسلم] عن [أبي هريرة] رضي الله عنه قال ، قال رسول الله صلى الله عليه وسلم "والذي نفسي بيده لو لم تذنبوا لذهب الله بكم و لجاء بقوم يذنبون فيستغفرون الله فيغفر لهم "

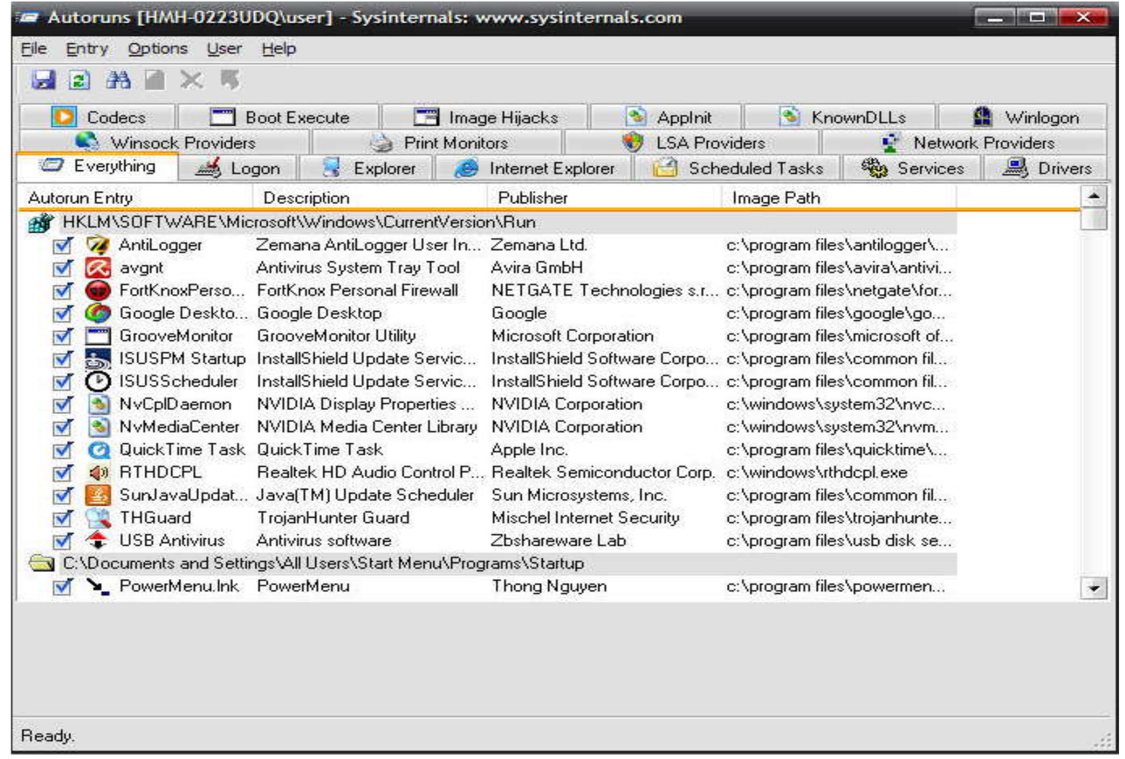
فلابد من الخطأ ولابد من التقصير وكلنا ذوو خطأ

من ذا الذي ما ساء قط * ومن له الحسنى فقط**

تريد مبرئا لا عيب فيه * وهل نار تفوح بلا دخان**

وجب أن نستدرك أخطائنا ، ونتفاعل مع كل خطأ بالتفكير ملياً في كيفية ارتكابنا له ، وكيفية عدم رجوعنا لارتكابه ، ولا يتبادر لأذهاننا كما يتبادر للبعض من حب الاستطلاع والتجربة ، فقد يكون الخطأ الذي تخطط عمله الأول ، وقد يكون الأول والأخيـر أيضـاً ..

احترامي وتقديري لجميع العقول النيرة ، التي تحاول بشتى الطرق عدل المسار التفكيري للمجتمعات العربية بكافة طبقاتها وخبراتها .



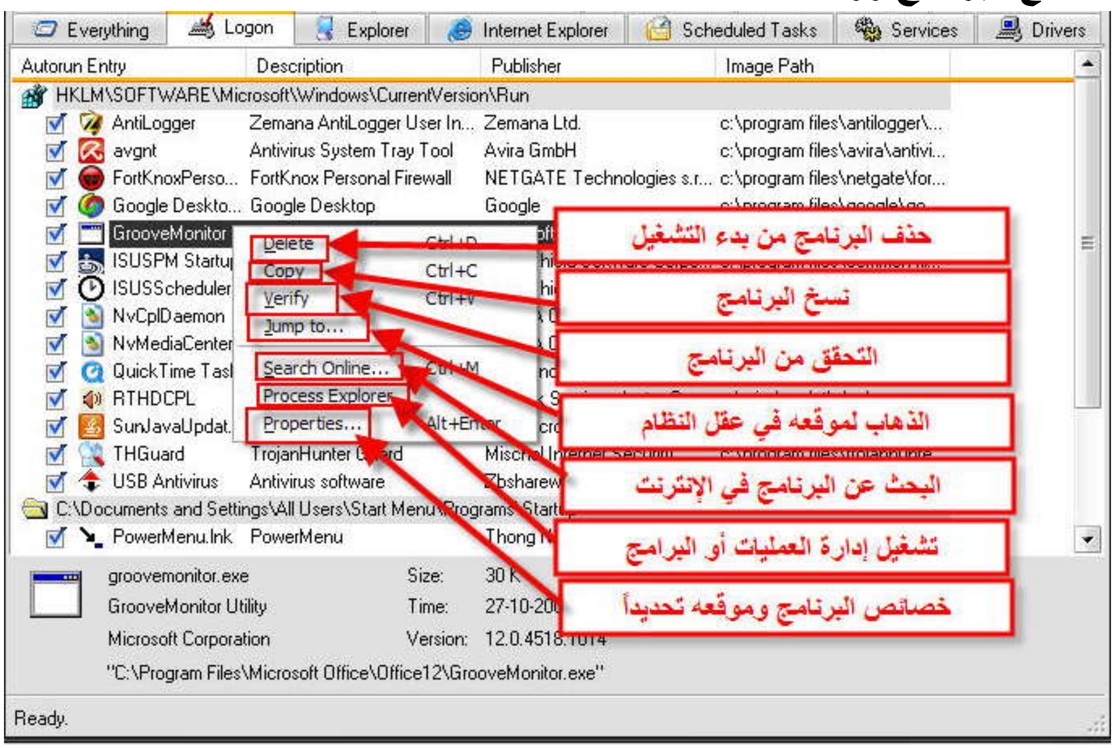
هذا هو البرنامج المطلوب ، سهل جدا في التعامل وسيتم تعريبه إن شاء الله وطرحه داخل المدونة ، وسيتم طرح شرح فيديو لكيفية معالجة جهاز أصابه إحدى ملفات التجسس بالاعتماد على هذا البرنامج .



قائمة Logon وهي البرامج التي يتم تشغيلها تلقائيا فور بدء النظام بالعمل ، وهي ما تهمنا في الغالب ولكن لا ضير في البحث عن اختلافات وإضافات في القوائم الأخرى .

نلاحظ أن قائمة البرامج الموجودة هي بالفعل ما ثبتناه بأنفسنا ، وجميعها نلاحظها تعمل فور بدء التشغيل ، ولكن ماذا لو كان هناك برنامج آخر في هذه القائمة لا يظهر بل يعمل في الخفاء ، هنا وجب علينا فحصه بشكل أدق ، وإرسالـه إلى مواقع الفحص على الانترنت ، ولكن سندع هذه الخطوات في درس منفصل إن شاء الله .

نكمل مع البرنامج ووظائفه ::

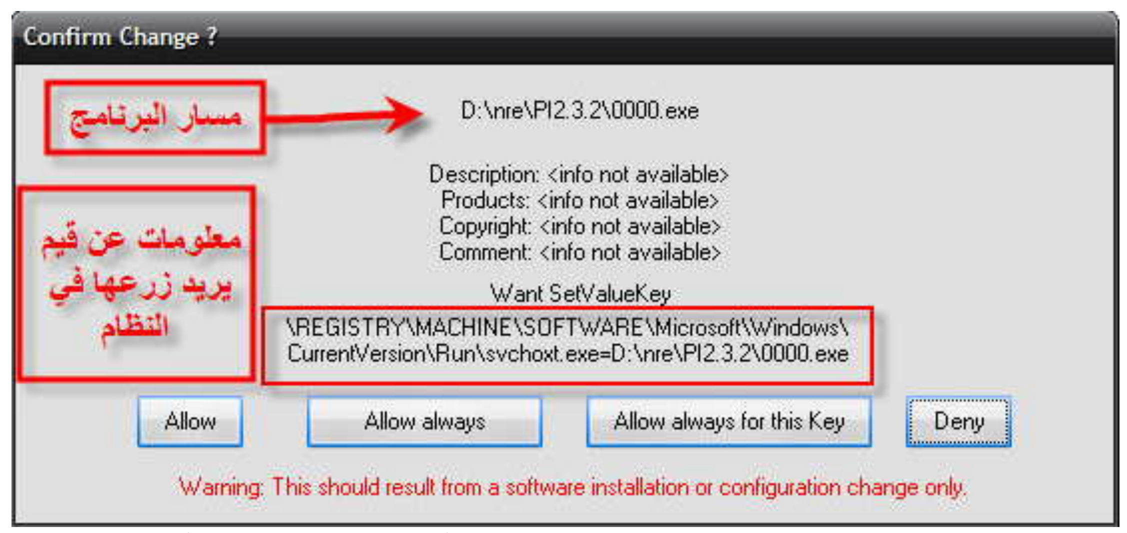


هذه القائمة توضح الأوامر المتوفرة ، ويجب أن يتم الإشارة إلى أن الحذف هو من عقل النظام ولكن سيستمر وجود الملف داخل الجهاز ، بالنسبة لنسخ البرنامج نستطيع نسخه على سطح المكتب ومن ثم رفعه على إحدى مواقع الفحص للتأكد من ماهيته ، أما التحقق من البرنامج فهو للأسف لا يهم كثيراً الآن لأن هذه العملية تم تجاوزها من قبل الهاكرز وجعلوا ملفات التجسس يتم التحقق منها على أنها سليمة بإضافة رموز التحقق داخل ملفات التجسس ، بالنسبة لخيار الذهاب إلى موقعه في عقل النظام فهذا لا يهمك كـ مستخدم عادي ، وننصح بعدم العبث بعقل النظام الداخلي لأنه يؤثر بشكل مباشر في النظام ككل ، بالنسبة لتشغيل إدارة العمليات والبرامج فهو لمتابعة تشغيل البرنامج من خلال برنامج إظهار العمليات ، والذي يفضل استخدام نسخة غير إدارة المهام المرفقة مع ويندوز XP ، وآخر قائمة وهي خصائص البرنامج تطلعنا على تفاصيل البرنامج وموقعه في الجهاز ، فإذا اكتشفنا أنه ملف فيروس لزم الذهاب إلى موقع الملف وحذفه ،فلو كان تروجان فسيتم حذفه بالكامل ، ولو كان دوده فللأسف من الصعب إزالتها بهذه الطريقة .

إلى هنا ننتهي من شرح البرنامج الأول في المراقبة ، ونتمنى للجميع تصفحاً آمناً وعلماً يفيد الأمة ، اللهم اجعلنا من صناع مجدها وقوتها .

البرنامج الثاني : System Shield

برنامج مجاني وهو بمثابة جدار ناري لعقل النظام ، سهل ووظيفته تتلخص في مراقبة البرامج التي تحاول زرع أو تعديل قيم في الريجيستري ، وعند حدوث ذلك يخبرك بهذا ويظهر لك مجموعة من الخيارات :



كما نلاحظ يحاول البرنامج 0000.exe زرع قيم في عقل النظام ، وفي مسار بدء التشغيل ، وتظهر أزرار الخيارات ومعناها كالتالي :

Allow :: اسمح بهذا .

Allow always : اسمح دائماً .

Allow always for this key : اسمح دائما لهذا المفتاح .

Deny: وهو الأهم ومعناه امنع ، طبعا هناك بعض البرامج التي قد تتطلب أثناء تثبيتها زرع أو تعديل قيم في النظام لذا أرجو الحذر ، واستمرار التجارب الفعلية وعمليات التطبيق .

وعملية المنع لا تعني إقفال البرنامج ، بل سيعمل البرنامج ولن يتم زرع القيمة التي تبدأه تلقائيا مع إعادة التشغيل فقط ، فحاول حينها فصل الانترنت والذهاب الى مسار البرنامج وحذفه ، وتأكد أنه لم ينسخ نفسه في مسار آخر .

تعد هذه العملية من عمليات المراقبة والتطهير ، فسنستخدم في عملية تطهير الجهاز من برامج التجسس برامج مشابهة .

البرنامج الثالث : Total Uninstaller

برنامج مميز ولكنه وللأسف غير مجاني ، ويعطيك ٣٠ يوماً لتجربة البرنامج وهي مدة كافية لنا ، لأننا لن نستمر في نظام التشغيل ككل أكثر من شهر ، وعليه فهذا البرنامج سيفيدنا جداً أثناء هذه العملية ، لنتابع معاً مميزات هذا البرنامج العملاق .

في حال قمت بتحميل برنامج ، وتشتبه فيه من أي شخص أو موقع على الانترنت ، وأردت فحصه ، ففي هذه الحالة لا يمكنك الفحص إلا بواسطة هذا البرنامج أو ما يشبهه ، فكرة البرنامج تقوم على أخذ صورة لكافة ملفات النظام مع التقاط صورة أيضا لعقل النظام ، ومن ثم تثبت البرنامج ، وتأخذ صورة أخرى للنظام وعقله .

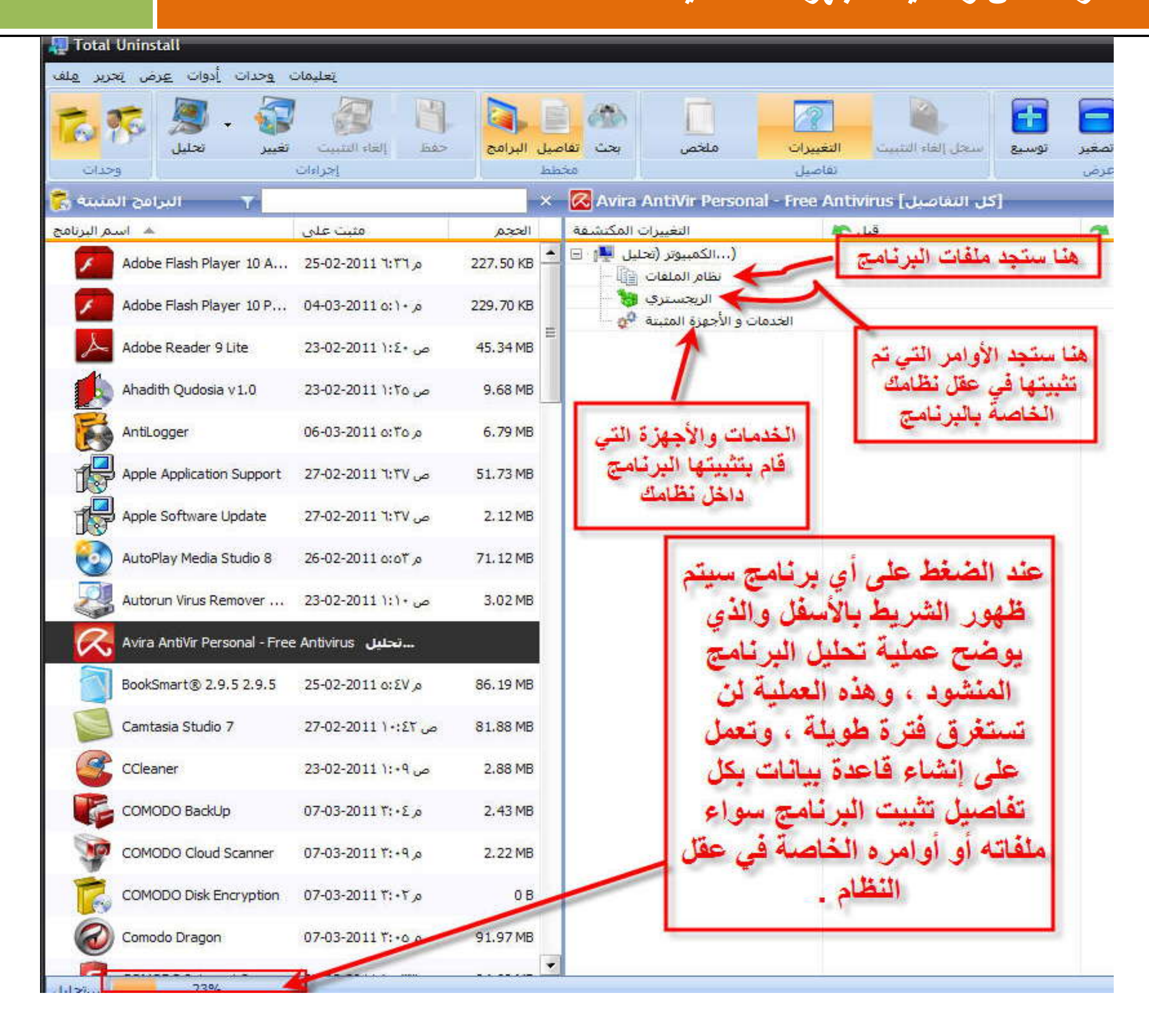
والخطوة الأخيرة هي مقارنة بين الصورتين ورؤية الاختلافات .

يفضل عند تنفيذ هذا الإجراء تطبيقه على الجهاز الوهمي ، وذلك حتى لا يكون ملف التجسس يحتوي على دودة معينة يصعب ملاحقتها وإزالتها .

بعد تشغيل البرنامج ستظهر واجهة البرنامج الرئيسية ، انتظر قليلاً ريثما يتم تحميل قائمة البرامج المثبتة فعليا داخل نظامك .



بعد الانتظار قليلاً سيتم ظهور قائمة البرامج بالشكل التالي :



كما نرى يتم تحليل البرنامج الذي نضغط بالماوس عليه وذلك حتى يتم تحليله ويستند البرنامج في التحليل على إظهار ٣ نتائج مهمة :

١ – يحلل الملفات التي قام البرنامج بتثبيتها داخل نظام الملفات الخاص بك .

٢- يحلل الأوامر التي أدخلها البرنامج في عقل نظامك .

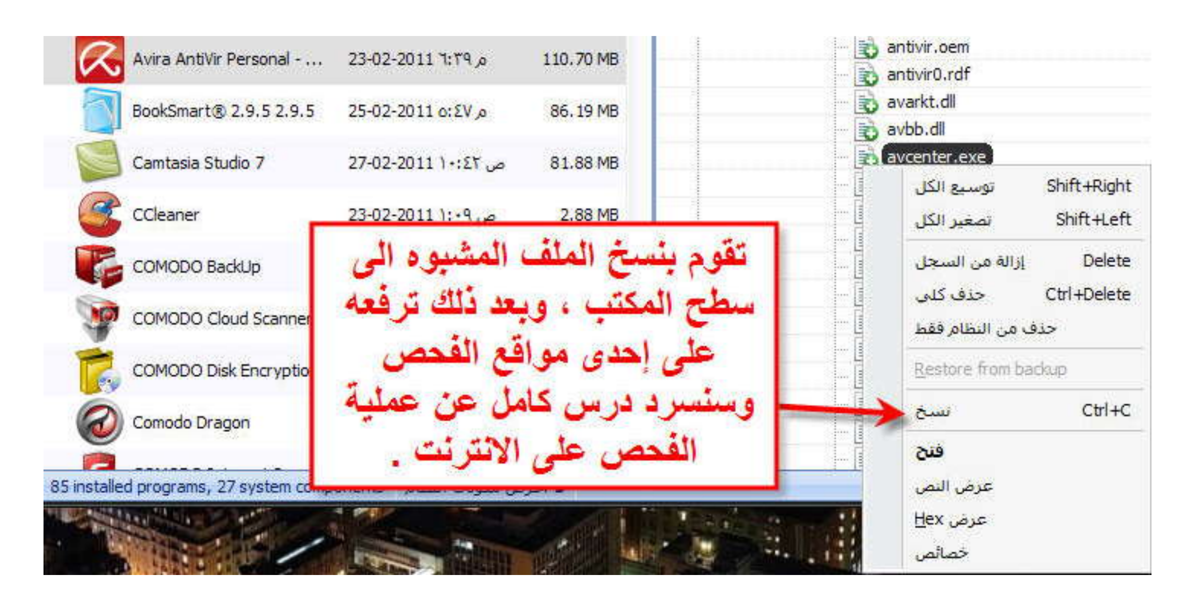
٣ – يحلل الخدمات والأجهزة التي قام بتثبيتها البرنامج داخل نظامك .

وعليه يظهر لك القائمة والتي تكون مزيجاً بين ملفات البرنامج التي ثبتها داخل جهازك ، مع الأوامر التي وضعها داخل عقل النظام ، مع إمكانية ظهور بعض الخدمات والأجهزة التي قام بتثبيتها البرنامج نفسه .

ما سنركز عليه في التحليل هو نظام الملفات بشكل أكبر ، ذلك لأن أوامر عقل النظام معقدة إلى حد كبير ، وقد يتم تغييرها بالشكل التي يرتئيه الهاكر لذا فمن

الواجب عليك أن تبحث داخل هذه الملفات عما تشك فيه أنه قد يكون إحدى برمجيات الهاكرز .

وحين ظهور ما تشك فيه ترسله لمواقع الفحص للتأكد أكثر ، كما في الصورة التالية :



طبعا من كثرة الملفات سيكون من الصعب العثور على الملف المشبوه بسهوله ، لذا سنبحث في البداية عن الملفات التي تحتوي الامتدادات التالية :

Exe , Scr , Pif , Com , Bat , Vbs

طبعا هذه الامتدادات في الغالب يستخدمها الهاكرز في عملية الدمج مع البرامج ، ولكن قد يكون البرنامج تم دمجه بأسلوب مختلف ومغاير ، لذا نرجو الحذر ، والتحميل من مواقع في قمة المصداقية والوثوق وعدم تحميل أي شيء إلا من مصادر موثوقة فالوقـــاية خير من العلاج .

طبعا هناك مئات إن لم يكن آلاف طرق الفحص ومعالجة تثبيت البرامج إلا أنها تعتمد نفس المبدأ القائل بأخذ صورة مبدئية للنظام بملفاته وهيكلية أوامر الريجيستري (عقل النظام) ومن ثم مقارنة النتائج بعد تثبيت البرنامج ، ورؤية الفروق التي حدثت بعد التثبيت .

ولكننا ننصح المستخدم العادي بشكل عام ، عدم الخوض في عملية الفحص والتدقيق إلا إذا تخصص في الأمر عن طريق الدورات البرمجية والتطوير الذاتي في هيكلية البرامج وكيفية زرع القيم والنظم وغيرها .

ذلك لأن الهاكرز يطورون آلياتهم بشكل يومي ؛ هذا بالإضافة إلى أن البعض قد يدمج عن طريق وسائل أخرى كثيرة في بنية البرنامج نفسه ولا يتم تشغيل ملف التجسس على الآلة الوهمية ولكن على الآلة الحقيقية يعمل .

لذا نرجو الحذر الشديـد ، خصوصا في مسألة البرامج ، وأعتقد أن الفترة التجريبية والتي قد تكون في الغالب ٣٠ يوماً جيدة جداً ، فأرجو الابتعاد عن مولدات السيريال والكراكات فأغلبها مدموج بـ تروجان وننصح بأن النظام لا يزيد عن الشهر ،؛ لذلك حمل من المواقع الرسمية لتلك البرامج أفضـل .

تستطيع أيضا من خلال البرنامج نفسه فحص سلوك تثبيت البرامج الجديدة عبر عمل مجموعة جديدة وإضافة البرنامج وحتى لو كان البرنامج مدموج بتروجان ففي حالة الاكتشاف ستتمكن من إزالة التروجان بشكل سهل جداً ، أرجو استخدام البرنامج والبرامج الشبيهة عند تثبيت البرامج الجديدة لزيادة الوعي وتطوير الذات فيما يخص سلوك البرامج المختلفة أثناء التثبيت وكيفية اكتشاف طرق الدمج .

تقديري واحترامي لكل من ينشر أفكار الحماية ، والبرمجيات التي تخص المستخدم العادي في منع المتطفلين .

دمتم بكل خير وصحة وسعادة ..

الدرس السابع : برامج وطرق فحص الاتصالات الداخلية والخارجية

هناك الكثير من البرامج التي تسهل علينا القيام بهذه العملية ، ولكن أود أن أذكر قبل أي شيء أمرين في غاية الأهمية والخطورة .

الأمر الأول أن حماية الجهاز الشخصي قد تكون داخلية إذن أن الحصن الخاص بنا قد نبنيه ولكن لأشياء داخل الجهاز ، أما جميع الأشياء التي تخرج أو تدخل من هذا الجهاز عبر بوابة الإنترنت هي معرضة للاختراق ، من وجهة نظري المتواضعة أن الانترنت الآن بالنسبة لصانعه الأساسي أصبح ماض بعيد ، وأصبح يستخدم تكنولوجيا جديدة أضخم وأفضل ، الناظر في التطورات المتلاحقة والمتسارعة يكاد يؤكد على أن التطوير يصلنا متأخراً جداً مقارنة بغيرنا ، ففي بعض البلدان الدقيقة تفرق ، وبعضها الثانية تفرق ، أما لنا نحن العرب فكل الدقائق و الأيام والعصور والأحداث لا تفرق ، فبدأنا نتجرع ما يريدوا سكبه لنا قطرة قطرة ، دون أن نحاول إنتاج أي شيء خــاص في هذا المجال .

صراحة أشياء غريبة أرى من واجبي أن أذكرها بداية حتى أؤكد أن عالم اليوم ليس كـالأمس ، بالنسبة لي (فلتعتبروني معقد) لا أؤيد وجود أي جهاز تكنولوجي في غرفة النوم مثلاً .. !!

يقول الخبراء :: أنه ومن عام ١٩٩٧ استطاعت بعض الشركات العالمية الخاصة بأجهزة مخابرات دولة مؤيدة للولايات المتحدة إنتاج جهاز يستطيع التجسس صوتيا على أي هاتف نقال في نطاق قد يصل إلى أكثر من كيلو متر ، ويستطيع البرنامج أيضا القيام بهذه المهمة حتى لو كان الجهاز مغلق . !!

هناك الكثيـــــر مما يؤكد على أن عملية التجسس في تطوير مستمر ، وأن التكنولوجيات التي وصلت بالفعل الأسواق الآن في قمة الرعب ، وتستطيع استهداف أي كان ، ويتم توزيعها بأسعار رخيصة وهي متاحة في دول تكنولوجية كالصين مثلاً وتباع على الأرصفة ، إلا أن الإقبال الكثيف من قبل جميع ذوي المناصب على حمل هذه الأجهزة يؤكد أنهم لا يكترثون أن تصل أي معلومة لأمريكا وحلفائها ، ولا يريدون محاولة ابتكار أي جهاز من شأنه السيطرة على المعلومات أو تشفيرها أو منع التجسس الذي قد يطول رأس الهرم أو قاع قاعه في دولنا العربية ..

من المهم أن نؤكد على أمور عدة في البداية أهمها على أن كل الكتاب جاء في وقت وللأسف الشديد يشهد تدهورا كبيراً على الساحة السياسية العربية ، فمن يريد التغيير للقمة العيش ، ومن يريد التغيير لمجرد التغيير ، وما من أحد يريد التغيير ليخدم الهدف الأكبر ، والحلم الأجدر بالسعي ورائه ..

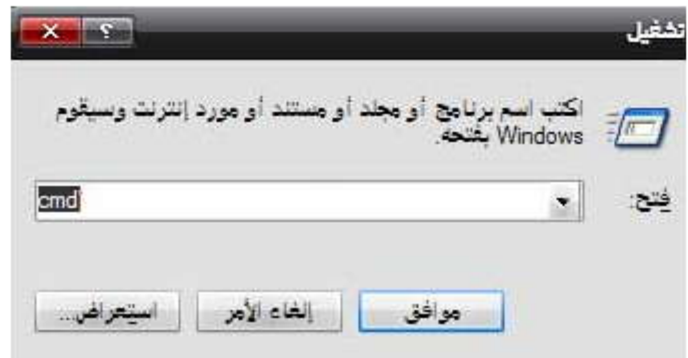
اعذروني إن كنت أطلت في إيضاح هذا الأمـر ،

ونتابع استعراضنا لآلية هذه المراقبة بالتالي ، يجب أن نعلم أن هناك طرق يدوية ، وطرق آلية ، الطرق اليدوية غير متعبة على الإطلاق وهي أساسا آلية كما سنشاهد ، ولكننا سنستخدم الإنسـان ونتعبه قليلاً في الأمور التالية .

وهذا الفحص طبعا يشمل جميع أنظمة التشغيل ، وسيستعرض جميع الاتصالات الصادرة والواردة ، وسيؤكد لك تقريبا هل جهازك مخترق أم لا .

نذهب لـ ابدأ ثم تشغيل كالصورة التالية ::





تظهر لدينا شاشة الدوس السوداء

فنكتب الأمر Netstat –an

وهو أمر إظهار جميع الاتصالات الصادرة والواردة .

```
C:\WINDOWS\system32\cmd.exe
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\user>netstat -an

Active Connections

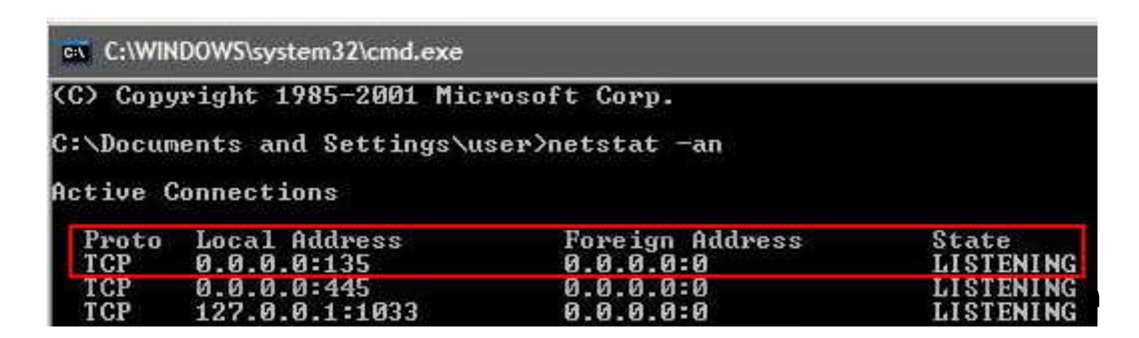
  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1033         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1063         127.0.0.1:1064         ESTABLISHED
  TCP    127.0.0.1:1064         127.0.0.1:1063         ESTABLISHED
  TCP    127.0.0.1:1065         127.0.0.1:1066         ESTABLISHED
  TCP    127.0.0.1:1066         127.0.0.1:1065         ESTABLISHED
  TCP    127.0.0.1:5152         0.0.0.0:0              LISTENING
  TCP    192.168.1.108:139      0.0.0.0:0              LISTENING
  TCP    192.168.1.108:2799     74.125.230.144:80      ESTABLISHED
  TCP    192.168.1.108:2824     174.37.106.5:80        ESTABLISHED
  TCP    192.168.1.108:2835     188.161.245.147:80     ESTABLISHED
  TCP    192.168.1.108:2836     188.161.245.147:80     ESTABLISHED
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:4500           *:*
  UDP    127.0.0.1:123          *:*
  UDP    127.0.0.1:1900         *:*
```

طبعا لن نركز إلا على القائمة الأخيرة :

وهي قائمة state وتعني حالة الاتصال .

حالات الاتصال كثيرة سنهتم بالحالتين ESTABLISHED + LISTENING

إذا وجدنا حالة LISTINING كالسطر التالي



```
C:\WINDOWS\system32\cmd.exe
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\user>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1033         0.0.0.0:0              LISTENING
```

وتعني العنوان المحلي ، مكتوب 0.0.0.0:135

وهذا يعني أن هذا الشباك مفتوح بالفعل داخل جهازك ، وينتظر اتصال ليتحول من حالة الانتظار إلى حالة الاتصال بالفعل أي إرسال واستقبال المعلومات .

0.0.0.0 تعني الآي بي

أما الرقم الذي يفصله نقطتين عنه (١٣٥) وهو البورت أو الشباك المفتوح بجهازك حتى تمر المعلومات من خلاله ، وهذا البورت مع بورتات أخرى يتم فتحه تلقائيا مع تثبيت نظام التشغيل ، وقد استخدمته بعض الديدان والفيروسات التي قد تصيب جهاز واحد في الشبكة فتحاول إرسال نفسها إلى باقي الأجهزة عليها .

المهم أن نعرف أن ما من معلومة تدخل أو تخرج من جهازك إلا عبر منفذ بورت شباك سمه ما شئت ، بعض البرامج تثبت منفذا خاصاً بها حتى تستطيع استقبال و إرسال المعلومات دون مضايقة ، ولا يمكن استخدام المنفذ في كثير من الحالات إلا ببرنامج واحد فقط يسيطر عليه ، بمعنى لا يمكن استخدام نفس المنفذ لأكثر من برنامج .

إذا وجدنا حالة ESTABLISHED

```
TCP    192.168.1.108:2824    174.37.106.5:80    ESTABLISHED
```

فنذهب إلى FORIGN ADDRESS

وهو العنوان الأجنبي الذي نقوم بإرسال أو استقبال المعلومات منه ، جدير بالذكر أنك من غير الممكن عمليا إذا لم تكن هاكرا بالغ الخبرة والدقة التسلل ومعرفة المعلومة التي خرجت منك ما هي السيرفرات التي وصلتها قبل أن يتم عرض الموقع لك ، كان هذا الأمر يأخذ وقتا طويلا ولكن مع السرعات الكبيرة لا تكاد تنهي كتابة العنوان حتى يظهر الموقع .

المهم أن هذا الآي بي ١٧٤.٣٧.١٠٦.٥

هو آي بي موقع IPMAP والذي أتصفحه الآن على جهازي لحظة تنفيذي هذا الأمر ، لو أخذنا هذا الرقم ووضعناه في المتصفح فمن المفترض أن تظهر لك صفحة موقع IPMAP ، وإذا لم يظهر لك أي موقع ، فتستطيع بكل بساطة الذهاب لنفس الموقع ،

[/http://www.ipmap.com](http://www.ipmap.com/)

وهو موقع خاص بإظهار معلومات عن المواقع والأفراد ، سيظهر لك حتى المدينة التي تم فيها الاتصال مع هذا الآي بي ، ولكن هدفنا هنا ، أن نعلم جيداً ما الفرق بين آي بي الموقع وآي بي الشخص ، في الغالب الفروق تكاد تكون بسيطة لا تلاحظ ، ففي البداية تضع الآي بي في المتصفح فإن فتح أي موقع ، فنذهب للآي بي الذي يليه ، وهكذا .

أما إن لم يفتح فنحاول الذهاب ومعرفة معلومات أكثر عنه .

وان كان آي بي شخص ، ولسنا نستخدم أي برنامج للاتصال عبر الانترنت ، إذن فجهازنا مخترق حتماً .

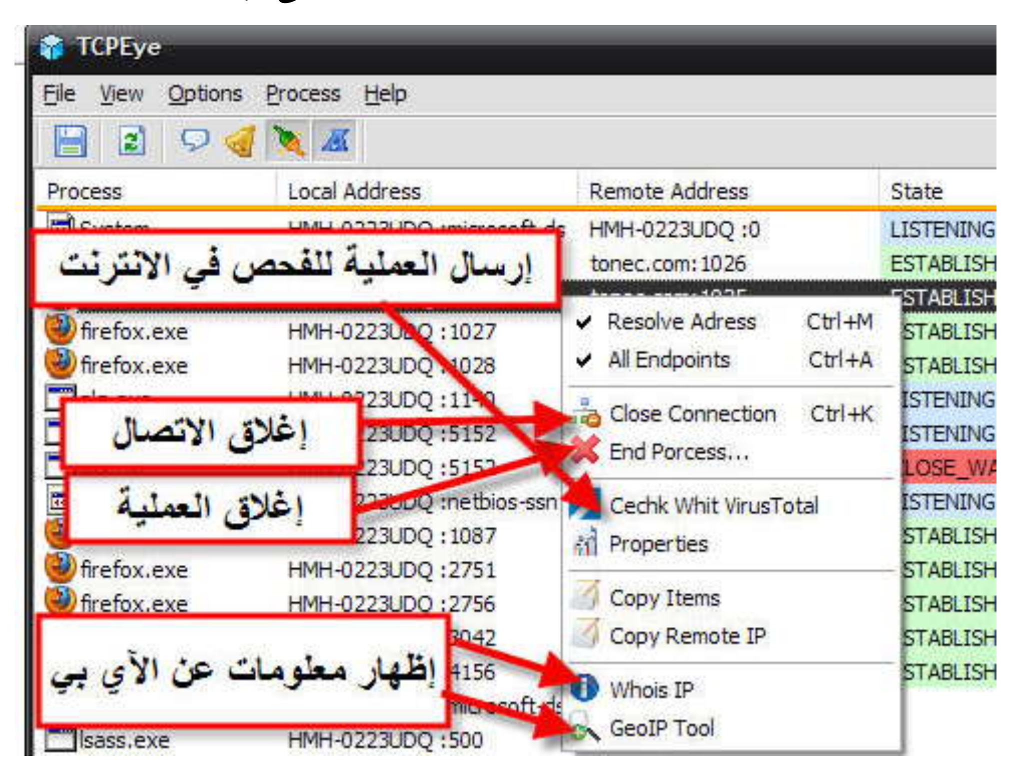
فالمفترض منك إيقاف عمل الانترنت والذهاب للآليات التي سيتم طرحها خلال هذا الكتاب بإذن الله في محاولة لإزالة الباتش من جهازك ، وإن لم تتمكن فلن يتبقى أمامك سوى عمل فورمات لنظام التشغيل الخاص بك .

برامج تسهل عملية فحص ومراقبة الاتصالات ::

سأقوم بشرح برنامج واحد لأن جميعها يتناول نفس الفكرة ، ولك الحرية في اختيار الأفضل .

برنامج TCPEYE

برنامج رائع في المراقبة يوفر عليك التعب في محاولة فتح الدوس مرارا وتكرار ، وبإمكانك استمرار تشغيله ومراقبة الحركة الخاصة بك على الإنترنت .



طبعا ملاحظة أخيرة أحببت أن أنوه إليها ، غالبا أطفال الهاكرز يخترقون بالبورت الافتراضي لبرامج الاختراق ، ولهذا ننتبه إلى المنفذ ، ونحفظه ثم نكتب في حبيب الجماهير الحالي والذي وفي إحصائيات حديثة يخزن معلومات البحث ومن أين صدرت تحديداً في قاعدة بيانات ضخمة لأكثر من ١٠٠ عام قادمة .

المهم أننا نكتبه ، ونكتب بجواره كلمة بورت ، إن لم نجد نتائج نكتب Port

وهكذا حتى نحصل على اسم البرنامج الذي يستخدم هذا البورت ، وفي الغالب كل برامج الاختراق لها بورت افتراضي واحد ، ولا يتم تغييره خصوصا من أطفال الهاكرز المنتشرين في المواقع العربية .

مثال ::

بورت 81 لبرنامج اختراق بفروست

3460 لبرنامج بويزون

الدرس الثامن : أساليب معرفة وتدمير المخترق

يجب أن نؤكد بداية أن ما سنشرحه داخل هذا القسم ليس من الضروريات في عملية الحماية ، ولكن قد تحتاجه للقضاء على بعض أطفال الهاكرز الذين ينشرون سمومهم داخل المنتديات العربية والمواقع المحترمة .

ما سيتم شرحه بخصوص تدمير المخترق بعض الطرق المستخدمة في كشف الحساب الخاص به ، ومن ثم إرسال هذا الحساب للشركة الأم والتي بدورها ستقوم بإغلاقه فورا وهذا الأمر سيفقده جميع ضحاياه الذين جمعهم .

هناك بعض العمليات المبتكرة الآن والتي يتم من خلالها اختراق أطفال الهاكرز عبر التروجان الخاص بهم ، ولكنها طرق معقدة لن نشغل المستخدم العادي بتعلمها لأنها أساساً عملية غير مهمة له .

الهوست :

هو العنوان الذي يتم إنشاؤه بواسطة الهاكرز بهدف اتصال ضحاياهم به ، وذلك لأن الآي بي يتغير في كل مرة ندخل فيها الانترنت ، وحتى نفهم هذه الآلية نشرح آلية الاتصال بالهاكرز حديثاً .

تم ابتكار طريقة الاتصال العكسي من قبل الهاكرز ، وذلك للحفاظ على الضحية المخترق حتى بعد الاتصال بآي بي آخر ، بمعنى لو فصلت الراوتر وأعدت تشغيله سيتم إعطائك آي بي جديد من شركة الانترنت ، ونفس الحال عند الهاكرز .

لذلك ابتكر الهاكرز طريقة الاتصال العكسي ، والتي يتم بواسطتها اتصال الجهاز الضحية بجهاز الهاكرز وليس العكس ، بمعنى عند تشغيل تروجان داخل جهاز أحد ما سيحدث التالي :

أولا : سيفتح التروجان بوابة لاستخدامها في عملية التجسس من قبل المخترق .

ثانيا : سيرسل للمخترق مكان تواجده بالتحديد على عنوان يتم برمجته داخله يعرف بالهوست .

ثالثا : تلقائياً يظهر جهاز الضحية داخل برنامج الاختراق عند الهاكرز ، وتعرف هذه العلمية بالاتصال العكسي ، فبدلا من أن يتم اتصال الهاكرز بأجهزة الضحايا ، تتصل أجهزة الضحايا بأجهزة الهاكرز .

تبدأ أولى أساليب المعرفة بالبرامج التي توفر لنا تتبعاً للاتصالات ففي طبقات الحماية ذكرنا وجوب تواجد جدار ناري ، وفي حال تشغيل تروجان سيظهر لك الجدار الناري رسالة تخبرك بأن برنامج كذا (حسب دمج الهاكرز) يحاول الاتصال بالهوست كذا (حسب الهوست الخاص به)

غالباً أطفال الهاكرز يكون الهوست الخاص بهم كالتالي :

xxxxxx.no-ip.com

مع التعويض عن xxxxxx بالذي اختاره عند صناعة العنوان الخاص به .

طبعا قد يختلف الهوست حسب ذكاء المخترق ، يجب أن تميز بين المواقع والهوستات أغلب هذه الهوستات تكون متصلة بشركات عالمية تقدم خدمة الهوست المجاني ، إلا أن المخترق قد يستخدم تكنولوجيات أخرى كثيره .

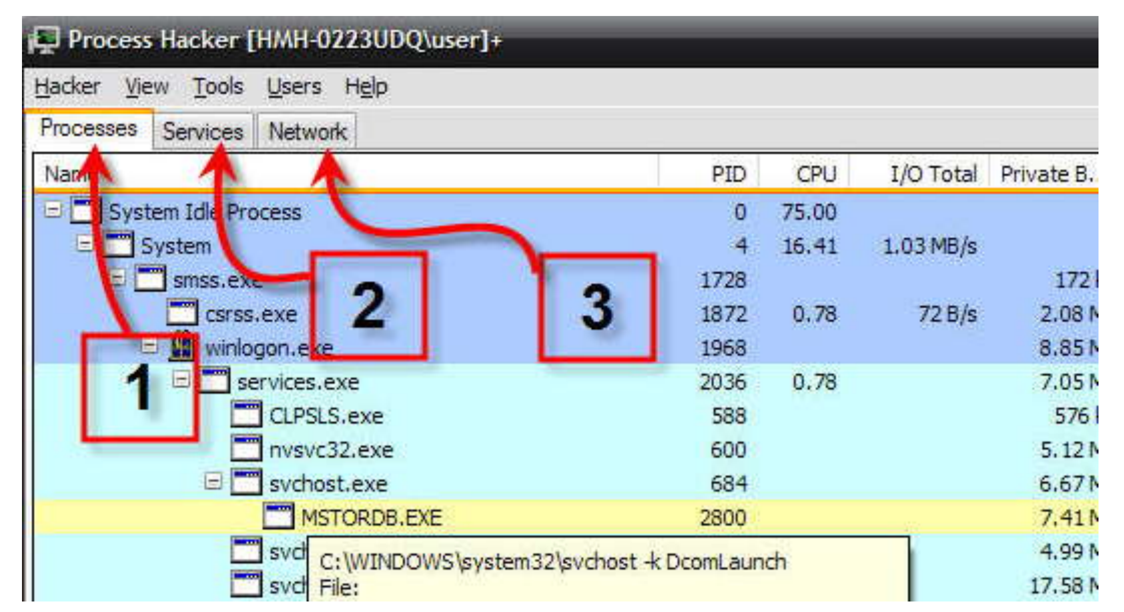
ولكن لو كان المخترق طفلا من أطفال الهاكرز واستطعنا الوصول للهوست بالطرق التي سيتم شرحها لاحقاً أيضاُ سيتم إرسال رسالة إلى الشركة التي أنشأ هذا الهاكر الهوست الخاص به ، وعليه ستقوم الشركة بإغلاق هذا الهوست بالكامل فوراً .

طرق أخرى لمعرفة الهوست ::

شرح برنامج Process Hacker

برنامج لمراقبة العمليات والاتصالات والخدمات داخل جهازك ، بمعنى أنه شامل ومميز جدا في عملية الرقابة المستمرة والتي يجب أن تنتبه باستمرار لها ، يظهر لك معلومات مفصلة جداً عن كل البرامج العاملة ، هذا بالإضافة إلى قائمة تظهر لك الاتصالات الموجودة وتتبع لأي برنامج بالضبط ، هذا والكثير مما سيتم شرحه من خلال الصور التالية ، ولكن لن نشرح إلا ما يهمنا فقط لأن البرنامج ضخم جداً ويحتوي على كثير من الأدوات ،

نتابع الصور ::



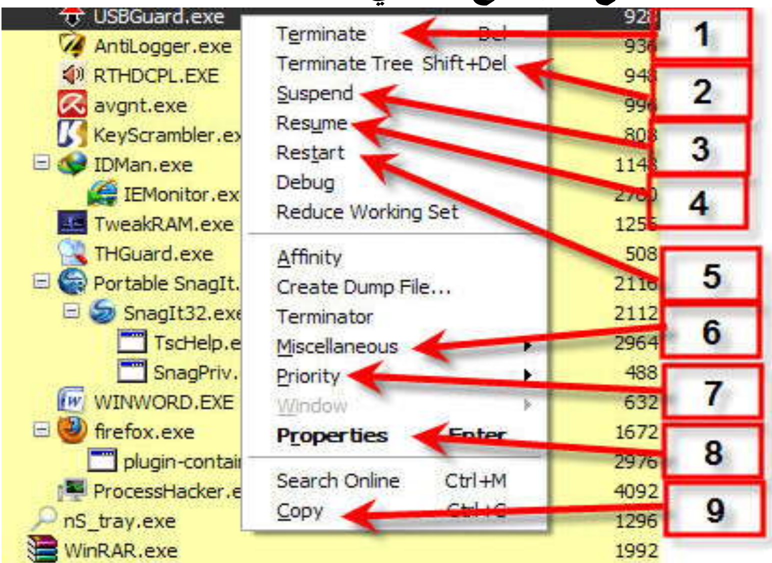
هذه هي الواجهة الرئيسية للبرنامج المميز ، وهو مجاني يتم تحميله من الموقع الرسمي ، وسيتم في قائمة المراجع وضع جميع وصلات البرامج بإذن الله .

١ – Processes : وهي قائمة العلميات أو البرامج التي تعمل بالفعل الآن داخل النظام .

٢ – Services : وهي قائمة الخدمات ، وهي قائمة غير مهمة لأن الهاكرز نادراً ما يدمجون التروجان بخدمة تعمل على الجهاز الشخصي .

٣ – Network :وهي القائمة المهمة الثانية بعد قائمة البرامج وقد تستخدمها في مراقبة الاتصال وتستغني عن برنامج TcpEye

عند تشغيل أي برنامج يظهر في هذه القائمة ، وعند الضغط عليه بالزر الأيمن تظهر خيارات التعامل مع البرنامج كالتالي :



١ – Terminate : إيقاف العملية ، إغلاق البرنامج .

٢ – Terminate Tree : إيقاف العملية بكافة ما تتبع .

٣ – Suspend : تجميد العملية .

٤ – Resume : إعادة تشغيل العملية بعد تجميدها .

٥ – Restart : إغلاق البرنامج ومن ثم إعادة تشغيله .

٦ – Miscellaneous : تحليل متقدم للبرنامج المستهدف .

٧ – Priority : قيمة البرنامج من أداء النظام ، تستطيع زيادة أداء بعض البرنامج لتسريعهم .

٨ – Properties : خواص البرنامج .

٩ – Copy : نسخ البرنامج .

ملاحظات هامة و طرق اكتشاف التروجانات

أغلق المتصفح الخاص بك ، وإذا وجدته من ضمن القائمة فتأكد احتواء جهازك على تروجان و الماسنجر كذلك .

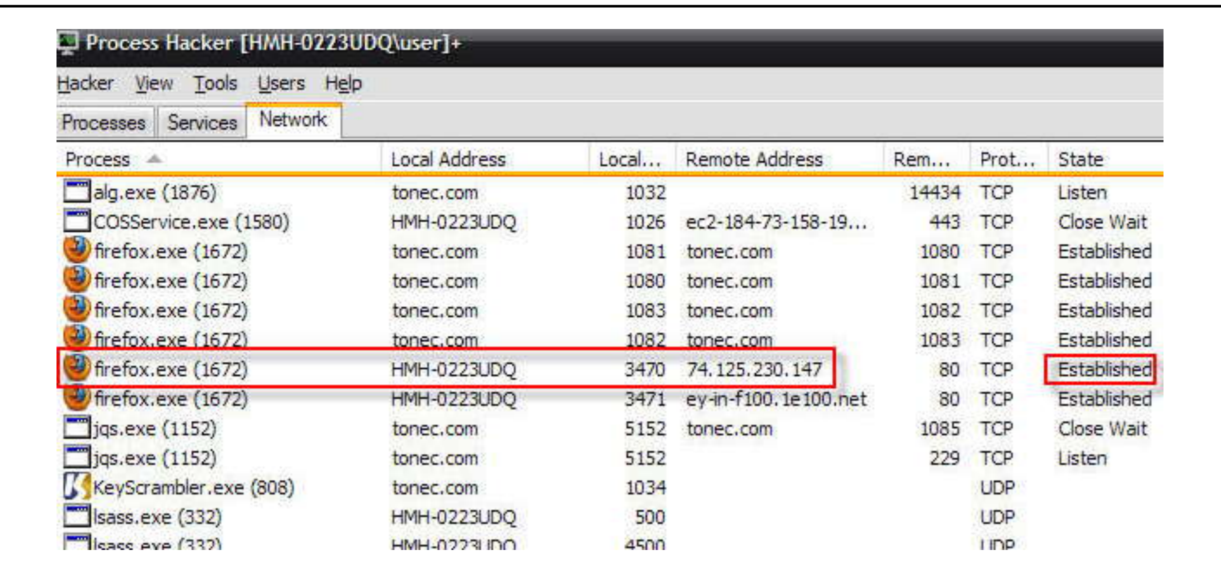
غالباً ستجد التروجان قد تم دمجه في المتصفح iexplore.exe

إذا قمت بعمل Terminate لعملية برنامج متصفح الانترنت أو أي برنامج آخر وأعادت تشغيل نفسها تلقائيا فاعلم انك حتما مخترق بـ تروجان .

حاول أن تغلق جميع البرامج تحت قائمة Explorer.exe

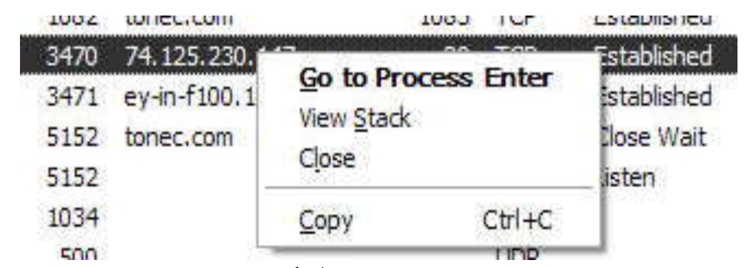
أي مستكشف الويندوز داخل ويندوز XP تحديداً ، وإذا وجدت برنامجا يعيد تشغيل نفسه فأغلق الانترنت فوراً .

عند عدم تمكنك من تتبع البرامج بشكل جيد ، اذهب لقائمة Network لتراقب الشبكة الخاصة بك ، وتتعرف على ما يحدث الآن من تبادل للاتصال بينك وبين عالم الانترنت ، ويعطيك البرنامج إمكانية إيقاف أي عملية أو أي اتصال كما سنرى في هذه الصورة التالية :



طبعا كما هو ظاهر أمامنا صورة البرنامج المستخدم للاتصال مع الآي بي الذي تم الاتصال به ، هذا بالإضافة إلى معلومات عن بورت الاتصال وحالته ، كما هو الحال في درس مراقبة الاتصالات .

تستطيع من خلال الضغط بالزر الأيمن على الاتصال المستهدف وظهور الخيارات في الصورة التالية عمل ما يلي :



Go to Process بمعنى اذهب إلى العملية أو البرنامج الذي يستخدم هذا الاتصال ، وهو في هذه الحالة برنامج **FireFox**

Copy تستطيع نسخ الآي بي ووضعه في المتصفح لمعلومات أكثر من خلال المواقع التي تظهر معلومات عن الآي بي .

في حال مراقبة الاتصالات ستجد آي بي المخترق أو الهوست الذي يستخدمه في برنامج **Process Hacker**

برنامج HeapMemView

برنامج مميز يتم من خلاله تحليل البرامج المدموجة دون اتصال إنترنت من أجل الوصول إلى الهوست ، وتتم هذه الطريقة كالتالي :

نغلق جميع البرامج ، وخصوصاً متصفحات الانترنت و الماسنجر .

نقوم بإيقاف الانترنت .

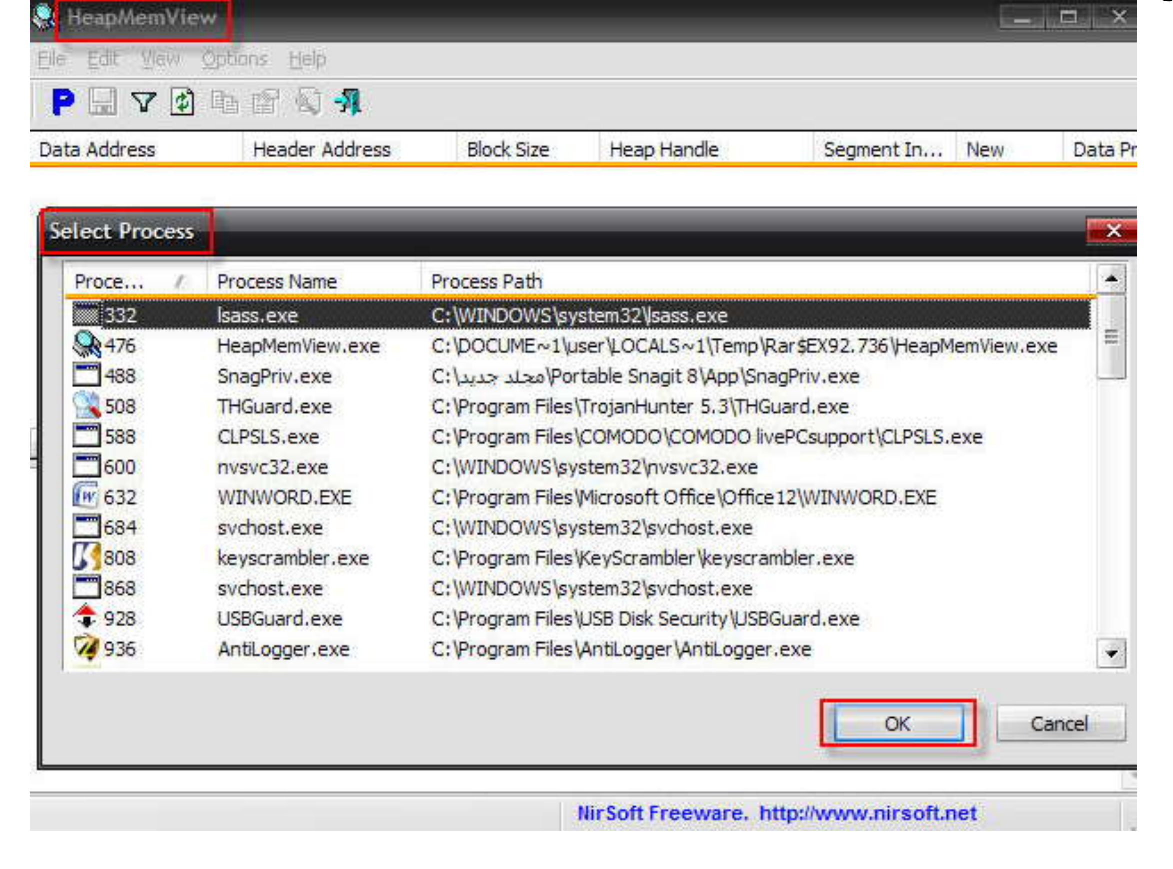
نشغل برنامج Process Hacker

نشغل البرنامج المشكوك في أمره .

غالباً سيتم ظهور المتصفح في قائمة البرامج العاملة ، مع أنك أغلقته سابقاً .

إن لم يظهر سيظهر أي برنامج باسم غريب أو جديد .

نفتح برنامج HeapMemView فتظهر القائمة التالية :



هذه هي الواجهة الرئيسية ستظهر قائمة Select Process

وتعني اختر عملية لتحليلها نؤكد على ضرورة إغلاق الانترنت ، والتجريب على النظام الوهمي .

نختار العملية المشكوك فيها ، ومن ثم يتابع البرنامج كالتالي ::

بيانات الأدرس	هدر الأدرس	ح	...بيانات المك	س	بيانات الملف
0x00034100	0x000340f8	112	0x00030000	0	S.o.f.t.w.a.r.e.\.M.i.c.r.o.s.o.
0x00034280	0x00034278	112	0x00030000	0	S.o.f.t.w.a.r.e.\.M.i.c.r.o.s.o.
0x00034360	0x00034358	112	0x00030000	0	....f.t.w.a.r.e.\.M.i.c.r.o.s.o.
0x001522c8	0x001522c0	112	0x00150000	0	....
0x00167848	0x00167840	112	0x00150000	0	....s.t.e.m.\.C.u.r.r.e.n.t.C.o.
0x02e71eb0	0x02e71ea8	112	0x02e70000	0	mohob-HKR_google.no-ip.info.....
0x000329c0	0x000329b8	120	0x00030000	0	@*...*...*...+.. +..P+..p+...+..
0x0015cc68	0x0015cc60	120	0x00150000	0	....a.l.r.p.c.:.[.D.N.S.R.e.s.o.
0x00382a00	0x003829f8	120	0x00380000	0	.*8..*8..+8.@+8.`+8..+8..+8..+8.

```
02E71EB0  6D 6F 68 6F 62 2D 48 4B 52 5F 67 6F 6F 67 6C 65   mohob-HKR_google
02E71EC0  2E 6E 6F 2D 69 70 2E 69 6E 66 6F 00 00 00 00 00   .no-ip.info.....
02E71ED0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
02E71EE0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
02E71EF0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
02E71F00  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
02E71F10  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
```

نستمر في قراءة الأسطر تنازلياً حتى نحصل على شبيه ما سبق ، ملفتين عناية الإخوة والأخوات من يقرأ هذا الموضوع ، أن النسخة التي أنزلها الأخ صاحب هذا الهوست في إحدى المنتديات التعليمية للهاكرز ملغومة وللأسف الشديد لذا أرجو رجاءاً حاراً من الجميع في المنتديات بشكل عام أن لا يثق كثيرا بأحد ، فقط اقرأ الشرح أما إذا أردت تحميل أي برنامج فانظر في النصائح التي سأضعها في درس في نهاية هذا الكتاب .

علماً بأن هذه الصورة تم سحبها من شرح فيديو للأخ الموهوب في إحدى المنتديات وكما ذكرنا كان البرنامج مدموجاً .

بعد حصولنا على الهوست الظاهر كالذي يظهر في الصورة السابقة نرسله إلى الايميل التالي مع نص الرسالة ، مثلا سنطبق على الهوست السابق في الصورة::

البريد المرسل إليه : **abuse@no-ip.com**

In this client No-IP : mohob-HKR_google.no-ip.info
This client is used for Hacking
please punish this client

I believe that you will take care about this problem

Thanks team NO-IP

الدرس التاسع : فحص البرامج على الإنترنت

الأجانب ، دائما ما نكرر البرامج والمواقع التي لا تحتوي أي موقع عربي قد يساهم في خلق إنترنت صحي للمستخدمين العرب ، وهذا يؤكد الإحصائيات القائلة أن أكثر المخترقين وللأسف الشديد هم من العرب ، جدير بالذكر أن هناك مؤسسات تدين بالعداء إلى العرب تعمل ليل نهار لاختراق الكم الأكبر من المستخدمين العرب لعدة أهداف ضخمة يأتي في مقدمتها خلق مجتمع يبحث عن الرذيلة ، وكم من فتاة وشاب تم إسقاطهم في وحل الخطايا بواسطة هذه الجماعات الحقيرة والتي وللأسف مقراتها بعض الدول العربية ، ليس هذا فحسب فأصبح لهم الآن قنوات تلفزيونية ومقرات وغير ذلك الكثير من سبل التأثير فينا إخوة وأخوات .

أرجوكم اعملوا على حماية أنفسكم ، وحماية كل من يعز عليكم فالأمر أصبح يتخطى المتعة بمشاهدة بعض قصص التجسس على الغير ، ويتخطى الكثيرين في محاولة مراقبة فلان أو علان ، يجب علينا أن ننشر فكر الحماية ونطور المؤسسات والجمعيات وندعم كل العقول التي من شأنها تطوير العقل العربي لمستقبل أفضل ، فالحرية التي يطالبونا بالتمسك بها والبحث عنها من وجهة نظرهم تبدأ من غرفة النوم ، وتنتهي عند انتهاء الشهوة .

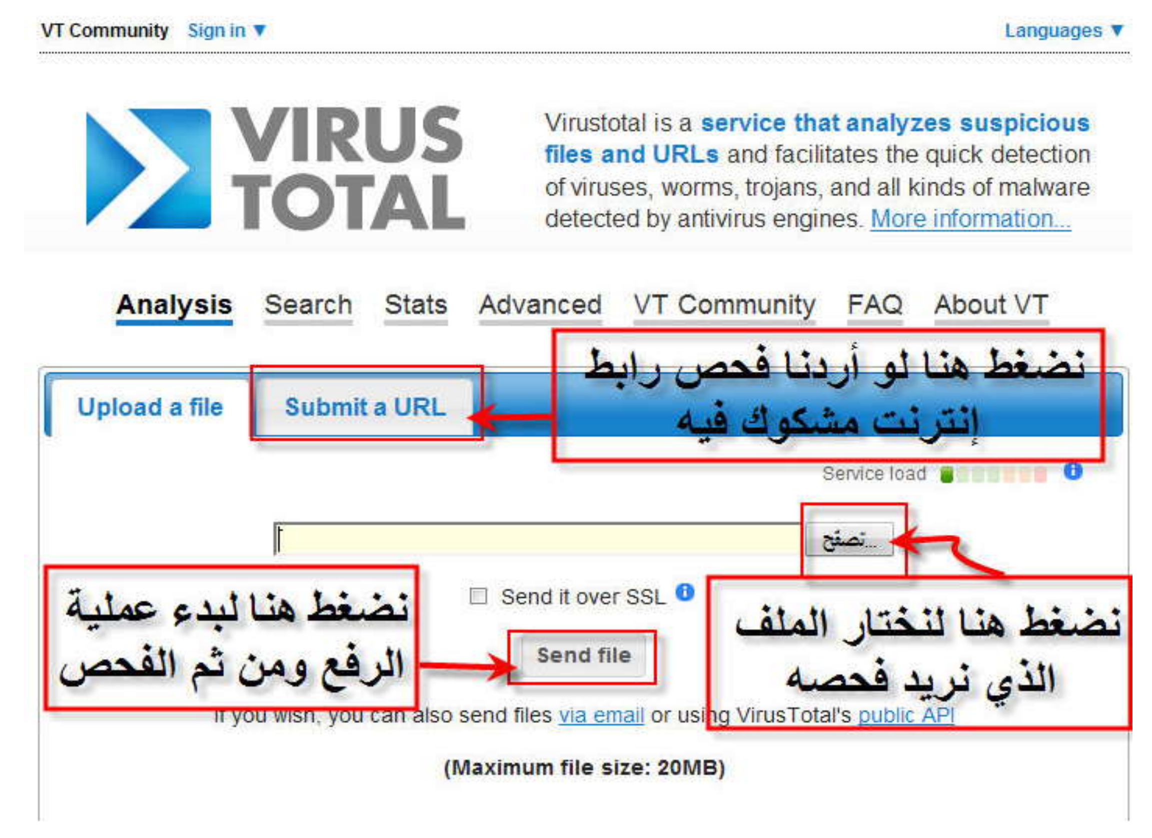
لا يهمهم فقر بعضنا ، ولا حقوقهم ، ولا استغاثاتهم ، ولو كانوا كذلك فأين هم من عشرات السنين عن قضية العرب المركزية فلسطيـن ، أين هم من المجازر اليومية والمآسي اللحظية التي تحدث على مستوى قارة أفريقيا تحديداً ، ولماذا يغضوا البصر حين ذكر المنظمات اليهودية والمسيحية التي ترتكب أبشع الجرائم في روسيا وتايلند وأمريكا الجنوبية وغير ذلك الكثيـر ،

لا أريد أن أقول المزيد فجميع من سيقرأ هذا الكتاب أعتقد أنه يعرفنا واقعنا ، ويتألم كما أتألم إن لم يكن أكثر ، كل لحظة تمر لن تعود ، فلننتهز وقتنا البسيط على هذه الأرض ، ونعمل على إنشاء مستقبل أفضل لمن سيعيش بعدما نغادر ، أم تريدوهم يبغضون هذه الحقبة التي نعيش هي وكل من عاش فيهـا .

الموقع الأول : Virus Total

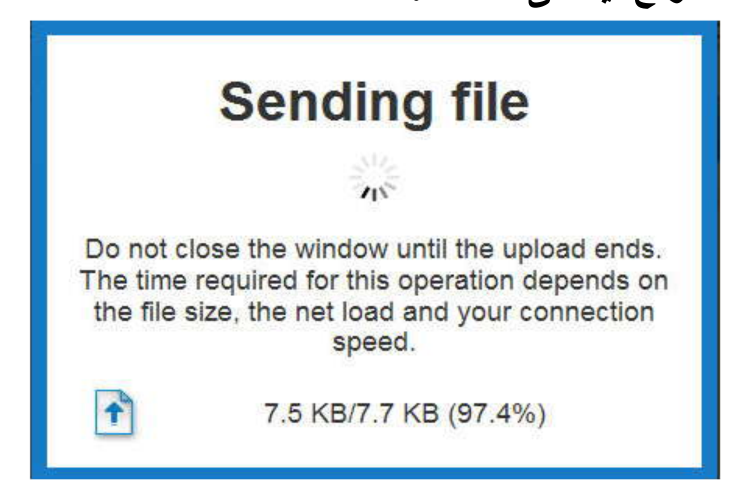
موقع مشهور جداً يتعامل مع أكثر من ٤٠ مكافح فيروس مشهور في العالم ، يتم فحص الملف المطلوب وإظهار النتيجة بدقة تقارب الفحص على الجهاز الشخصي ، يرسل التقارير أول بأول لشركات الحماية والتي بدورها تحلل الملفات والبرامج وتكتشف القيم التي يتم تشفيرها من قبل الهاكرز .

/http://www.virustotal.com



كما نرى نختار الملف المشكوك فيه ، ومن ثم نضغط على زر Send File

ليتم إرسال الملف للموقع ليتسنى فحصه .



نلاحظ ظهور القائمة السابقة والتي تخبرك بضرورة عدم إغلاق الصفحة ليتم انتهاء رفع الملف من جهازك إلى الموقع ومن ثم الفحص على البرامج الموجودة في الموقع . تنتظر قليلا فتظهر الصفحة التالية ::

File name: sawwwwa.exe
Submission date: 2011-03-17 21:24:34 (UTC)
Current status: queued (#1)

إنتظر حتى تظهر النتيجة

هنا يخبرك بأن تنتظر حتى ينتهي من الفحص ويظهر لك النتيجة بالكامل كما سنرى لاحقاً ، ونسبة اكتشاف الملف والقيمة المكتشفة في كل مكافح فيروسات .



0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is goodware. 0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is malware.

File name: sawwwwa.exe
Submission date: 2011-03-17 21:24:34 (UTC)
Current status: finished
Result: 42/ 43 (97.7%)

Compact

Antivirus	Version	Last Update	Result
AhnLab-V3	2011.03.18.00	2011.03.17	Win-Trojan/Poison.8192.AF
AntiVir	7.11.4.248	2011.03.17	BDS/PoisonIv.A.8704
Antiy-AVL	2.0.3.7	2011.03.17	Backdoor/Win32.PoisonIvy.gen
Avast	4.8.1351.0	2011.03.17	Win32:Tiny-ADY
Avast5	5.0.677.0	2011.03.17	Win32:Tiny-ADY
AVG	10.0.0.1190	2011.03.17	BackDoor.Generic9.MQL
BitDefender	7.2	2011.03.17	Trojan.Keylog.ZKT
CAT-QuickHeal	11.00	2011.03.17	Backdoor.Poison.pg
ClamAV	0.96.4.0	2011.03.17	Trojan.Downloader-24568
Commtouch	5.2.11.5	2011.03.17	W32/Agent.G.gen!Eldorado
Comodo	8015	2011.03.17	Backdoor.Win32.Poison.NAE
DrWeb	5.0.2.03300	2011.03.17	BackDoor.Poison.[illegible]
Emsisoft	5.1.0.2	2011.03.17	Virus.Win32.Poison!IK
eSafe	[illegible]	2011.03.17	[illegible]
eTrust-Vet	36.1.8221	2011.03.17	Win32/SillyDl.DQU
F-Prot	4.6.2.117	2011.03.17	W32/Agent.G.gen!Eldorado
F-Secure	9.0.16440.0	2011.03.17	Backdoor:W32/PoisonIvy.GI

طبعا الموقع مميز ، ولكن لا يمكن الاعتماد عليه أو على غيره وذلك لأنه لا يحتوي سوى طبقة مكافح الفيروس ، أي أن النتيجة قد يتجاوزها الهاكرز حينما يقوم بتشفير التروجان الخاص به ، إلا أن أغلب التروجانات التي يتم تشفيرها لا يمكن أن تتجاوز جميع مكافحات الفيروس إلا في حالات بسيطة جداً .

الموقع الثاني : ThreatExpert

http://www.threatexpert.com

موقع للفحص أيضا ، ويختلف عن سابقه بإعطائك تقرير مفصل عن نشاط البرنامج لو تم تشغيله على النظام ، وما الذي سيحدث تحديداً .

يجب التسجيل في الموقع من خلال الذهاب إلى Sign Up

Your Details:

*User name: TornhearT

*Type password: ••••••

*Retype password: ••••••

*E-mail address: z83@live.com

يتم التسجيل في الموقع

Note: Your privacy is ensured by our Privacy P

Optional Information:

First Name: ham

Last Name: hij

Company: Gaza

Address: Gaza

Phone/Fax:

If you would like to be contacted to receive more information about ThreatExpert

I would like to be contacted

Note: Your privacy is ensured by our Privacy P

التسجيل عادي كأنك تسجل في منتدى

Type the characters you see in this picture:

4L88R

*Type chara 4l88r

نسجل عادي بأي معلومات ، ثم نكمل بعد نجاح العملية نضغط على

Add sample

Browse/Search My Reports

Search:

Got a New Sample to Submit? Follow here

Results 1 - 1 of 1

فتظهر هذه الصفحة

Submit Your Sample To ThreatExpert

File to submit: (file size limit is 5Mb) تصفح...

1

Your E-mail address: hmh321@gmail.com

2

Your privacy is ensured by our Privacy Policy.

To submit your sample, you must read and agree to ThreatExpert Terms and Conditions:

3

I agree to be bound by the Terms and Conditions

The progress bar will track your upload:

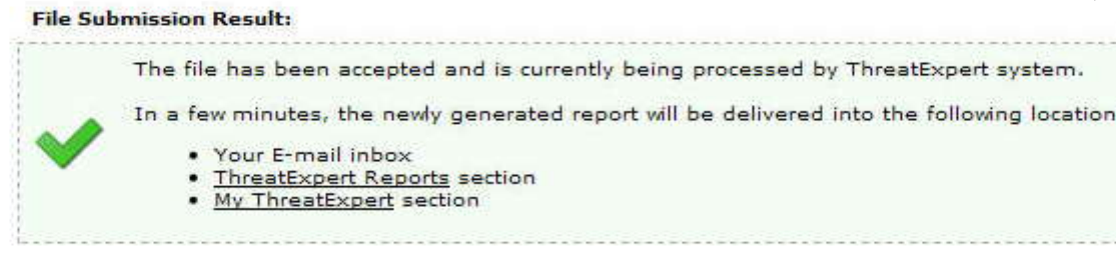
Submit

١ – اختار الملف المراد فحصه .

٢ – اختار الايميل الذي تريد لإرسال التقرير إليه .

٣ – اضغط على المربع لتوافق على شروط الموقع .

ثم اضغط زر **Submit**



رسالة تخبرك بنجاح عملية الإرسال ، وان تنتظر قليلا ريثما يتم إرسال التقرير .

شرح التقرير :



Submission Summary:

- Submission details:
  - Submission received: 17 March 2011, 19:05:51
  - Processing time: 7 min 10 sec
  - Submitted sample:
    - File MD5: 0xA0C6218FD97AA4D539B4578381D6BD8D
    - File SHA-1: 0xF412C4CED1774A3275411FEBCB89333DB53825A8
    - Filesize: 7,680 bytes
    - Alias:



      - Backdoor.Ciadoor!rem [PCTools]
      - Backdoor.Ciadoor [Symantec]
      - Backdoor.Win32.Poison.pg [Kaspersky Lab]
      - BackDoor-DSS.gen.a [McAfee]
      - Troj/Keylog-JV [Sophos]
      - Backdoor:Win32/Poison.M [Microsoft]
      - Virus.Win32.Poison [Ikarus]
      - Win-Trojan/Poison.8192.AF [AhnLab]

Registry Modifications

- The following Registry Key was created:
  - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Se
- The newly created Registry Values are:
  - [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active S
    - StubPath = "%System%\sxxx.exe"

    so that sxxx.exe runs every time Windows starts
  - [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
    - svchoxt.exe = "%System%\sxxx.exe"

    so that sxxx.exe runs every time Windows starts

معنى هذه الرسالة أن البرنامج المذكور اسمه سيتم تشغيله تلقائيا في كل مرة يتم تشغيل النظام .

يحتوي التقرير على معلومات أخرى ، ولكن الأفضل الاعتماد على الموقع التالي :

الموقع الثالث : **Anubis**

http://anubis.iseclab.org

البيانات حتى ولو كان التروجان مشفر ، وهو موقع يستخدم على نطاق كبير جداً ، وأصبح يمثل رادع لكثير من أطفال الهاكرز ، يطور نفسه بشكل مستمر مثلما الهاكرز يطورون أنفسهم ، وعليه فإنه يعتبر الأفضل على الاطلاق كما سنرى.

Anubis: Analyzing Unknown Binaries

Home | Advanced Submission | Clustering | News | About | Sample Reports | Links

Choose the subject for analysis

For analyzing Javascript and Flash files try Wepawet.

File: (max. 8MB) — Choose the file that you want to analyze. The file must be a Windows executable. (details)

URL: — Choose the URL that you want to analyze. The URL will be analyzed in Internet Explorer. *Note: We will not analyze a binary that you provide via this URL. We will merely use a browser to download or similar attack!*

http://

Get a priority boost

Enter the code that you see in the image on the left and your submission will be analyzed before all auto

Submit for Analysis

1 لإختيار الملف

2 لو أردت فحص رابط

3 اكتب الرمز

4 اضغط هنا

كما هو واضح في الصورة ، نختار الملف المراد فحصه ، ومن ثم ندخل الرمز ، ونضغط على زر **Submit for Analysis**

وننتظر قليلاً ليظهر التقرير ، وطبعا قد يطول ظهور التقرير لأن الموقع عليه ضغط شديد جداً من قبل الكثيرين .

شرح التقرير الظاهر :

Task Overview

Task ID:	10a0233d6b8c804349de76d351eb6a673
File Name:	sawwwwa.exe
MD5:	a0c6218fd97aa4d539b4578381d6bd8d
Analysis Submitted:	2011-03-17 21:50:24
Analysis Started:	2011-03-17 21:50:26
Analysis Ended:	2011-03-17 21:54:51
Created New Analysis Report:	Yes
Available Report Formats:	HTML XML PDF Text
Download Files:	traffic.pcap

من المفضل اختيار نوع HTML لوضوح التقرير فيها بشكل اكبر .

بعد الضغط سنعرف كل مايحدث عند تشغيل البرنامج على آلة دون الحاجة إلى وجود آلة ، فالموقع في هذه اللحظة يشغل البرنامج على آلة وهمية ويرصد جميع النشاط الخاص بهذا البرنامج ، كالتالي :

- Ikarus Virus Scanner

Virus.Win32.Poison (Sig-Id:1518180)

يفحص الموقع الملف على مكافح فيروسات قوي هو Ikarus

ويظهر النتيجة وإن كان مشفر لا يتم اكتشاف أي قيمة فنتابع قراءة التقرير .

إذا ظهرت هذه القيمة معناها انه ينسخ نفسه ليعمل تلقائيا بعد إعادة التشغيل وهو من مميزات التروجان

- Registry Values Modified:

Key
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKLM\Software\Microsoft\Active Setup\Installed Components\{75F37CE3-E146-AE46-3285-1C30FD8A1A57}

كما نلاحظ في تغييرات عقل النظام ، فهو يعدل أو يضيف قيمة جديدة له في عقل النظام ليخبره بأن يشغله فور تشغيل النظام تلقائياً ودون إذن من مستخدم النظام .



هذا أهم ما في الموضوع وهو الهوست ، ويظهر في قائمة Network Activity

و أيا ما يكون الهوست فهو في الغالب تابع لإحدى الشركتين العملاقتين :

No-IP

DynDNS

وفي كل الحالات حاول إرسال الرسالة التي تم ذكرها

للبريدين التاليين :

abuse@no-ip.com

abuse@dyndns.com

دمتم بكل خير وصحة وسعادة ،

وإن شاء الكريم ، سيتم إنشاء نسخة أخرى من الكتاب تحوي على القسم الخاص بالاختراق ولكن بعد فترة بسيطة وذلك لانشغالي الشديد هذه الفترة ، لم أرد تعطيل إصدار الكتاب أكثر من ذلك ، فقد نسبق طفل من أطفال الهاكرز بلحظة يقرأ من خلالها أحد الإخوة أو الأخوات الكتاب ويحمي نفسه ، صدقوني سأكون حينها قد أخذت المقابل ، وأي مقابل .

تقديري واحترامي للجميع .

وأرجو تزويدي من الإخوة والأخوات المتصفحين وإعلامي بأي خطأ أو إضافة ليتم وضعها في الإصدار الجديد .

وفقكم الله وسدد خطاكم .

القسم الثالث : نقاط ضعف المستخدمين

الدرس الأول :

الانتشار عبر المجموعات ، المحادثة ، المشاركة .

يستطيع الجميع أن يتذكر وفي بداية استخدامه للإنترنت أنه استقبل ومن أطراف عديدة برامج لا حصر لها ، بدءا من برامج عادية كانت تعمل عند تشغيلها بشكل اعتيادي ، أو عند الضغط عليها تتبخر وكأنها لم تكن موجودة ، أو بعد تشغيلها تظهر رسالة خطأ ، وغير ذلك الكثير من الأمور والتي تهدد استخدامنا لهذا العالم النافع في غالبه ، والذي بنى الكثيرين عليه عمله ، وتواصله مع العائلة والأصدقاء والأخوة وغير ذلك الكثير .

لذا فلا بد أن نستخدم الانترنت ، والحاسب بشكل عام ، ولا بد أن نحمل البرامج التي لا نستغني عنها ، وفي هذا القسم سأوضح من خلال الدروس القادمة بإذن الله كيف يمكن تحميل البرامج دون خوف ، ومن مصادر غاية في الوثوق ، هذا بالإضافة إلى إغلاق بعض نقاط الضعف لدى بعض المستخدمين .

أكيد مر عليك ، أن دخلت إحدى المجموعات فوجدت قائلاً يقول برنامج حديث يفتح لك جميع القنوات المشفرة ، أو آخر يقول برنامج يفك الحظر غصب ، وآخر يقول أعظم برنامج في التجسس على من معك على الماسنجر أو غير ذلك من البرامج المغرية والتي نزلتها أكيد وحاولت التعامل معها ، فوجدت أن كل ما قيل عبارة عن خيال ، أو اكتشفت أن البرنامج يعطيك رسائل خطأ عند أي عملية تقوم بها .

فما هو الحل لاستخدام هذه البرامج ، ذكرنا سابقا وفي مناسبات عديدة كلمة وهمية ، وهذه البرامج ما هي إلا برامج وهمية ، تم إنشائها خصيصا لإغرائك فقط بتحميلها ، وعندما تحملها وللأسف الشديد يتم اختراقك بكل سهولة ، لأن من يصنعها يدمج معها تروجان ويشفره جيداً ليتخطى بذلك طبقة الحماية الوحيدة التي لديك ، إياك أن تصدق كل ما تسمع ، ولا تثق سريعاً في أي عبارة من أي شخص .

فقد تجد فجأة أخيك أو صديقك يتكلم معك بأسلوب غريب ، ويرسل لك ملفاً غريباً على برامج المحادثة ، حينها قد يكون حدث إحدى ثلاثة أمور :

الأول : انه وفعلا هذا برنامج جيد ويتم إرساله من الشخص على الطرف الآخر .

الثاني : أن أيميل صديقك تم اختراقه وهذا الهاكر يحاول إغرائك ليخترقك أنت الآخر .

الثالث : أن صديقك قد تعلم الهاكر وجاء ليطبق عليك لأنه يعلم أنك أضعف حلقة في الإنترنت .

وفي كل الحالات حاول عدم القبول ، اعرف اسم البرنامج وابحث عن الموقع الرسمي الخاص به .

وان كان البرنامج يجب شراؤه ، تابع معي كيف ستتعامل مع هذا الموقف .

أولا ستكتب على محرك البحث قوقل العبارة التالية :

Site:mediafire.com ثم اسم البرنامج

ومعنى ذلك ابحث فقط في موقع Mediafire وهو موقع مشهور لتحميل الملفات عن هذا البرنامج ، وحاول أن تدخل على نسخة قديمة بعض الشيء لعدة أسباب ، السبب الأول هو حتى لو كانت مشفرة فقد تم اكتشاف تشفيرها لأن مكافح الفيروس يعتمد على تقارير الفحص في أجهزة المستخدمين .

فلو أردنا البحث مثلا عن برنامج AntiLogger

فستكون العبارة: Site:Mediafire.com AntiLogger

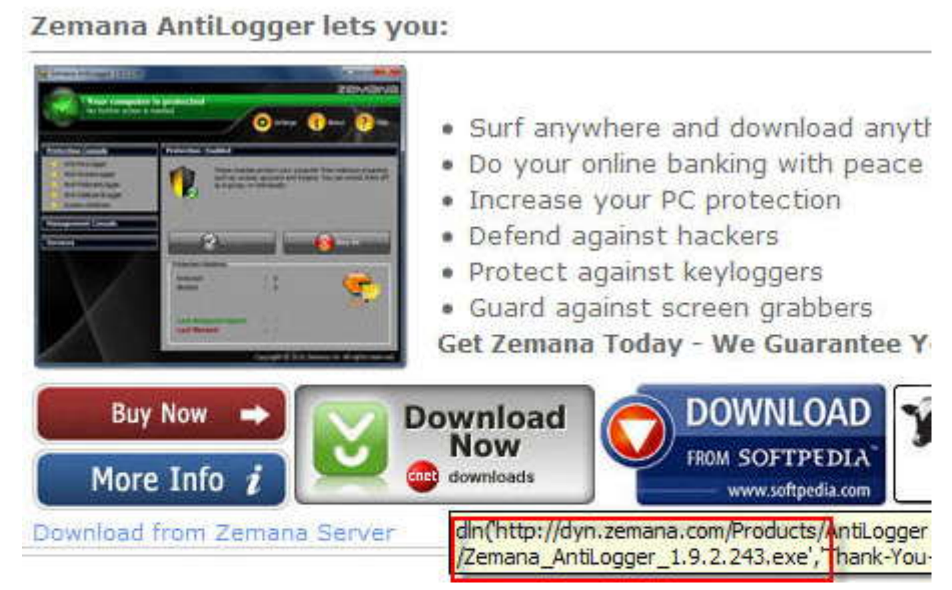


حاول أن تفحص البرنامج أيضا بعد تحميله على موقع **Virus Total** ، وموقع التحليل **Anubis** ، بعد ذلك تفحص البرنامج على الجهاز الوهمي وتمرره على الطبقات التي تم الإشارة إليها ، ومن ثم تستخدمه .

حاول أن تحرص جيداً حين استخدامك لعالم الانترنت فهو عالم لا يرحم ، وسيستخدم الهاكر الذي سيحاول اختراقك جميع ما يخصك من معلومات ، وقد يستخدم بريدك الالكتروني في اقتناص كل الأشخاص الذين يثقون بك من عائلة وأصدقاء وغيرهم .

فلا يستهين أحدكم في موضوع الحماية ، فقد يستخدمك الهاكر كـ جسر للوصول لأعز الناس عليك ، وكل من يثق بك ، وتثق به ، إياك أن تقصر في حماية نفسك ، وتخطي أسلوب واحد من وسائل الحماية ، وإياك أن يتم إغرائك بسهولة ، حاول التدقيق في أسلوب ومساعي كل من يعطيك دون مقابل ، حتى أنـا لا أعطيك دون مقابل فأنا أطمع لأجر الرحمن ، ولدعائك هذا بالإضافة إلى أني نشرت اسمي ومسئول عن أي ملف يتم نشره لو كان يحتوي على أي ملف تجسس ، تابعوا معنــا إخواني وأخواتي لدعس جميع الملغمين في المواقع العربية ، جعلهم الله عبرة وآية .

لمعرفة آخر إصدار لأي برنامج ندخل إلى موقعه الرسمي ونبحث عن **Download** أو **Buy** أو أي عبارة تحتوي كالآتي :



نلاحظ أن آخر إصدار هو **1.9.2.243**

فنبحث في أقرب إصدار إلى الإصدار الأخير ، أي قديم إلى حد ما وليس كثيرا جدا بحيث يكون البرنامج أكل الدهر عليه وشرب .. :)

الدرس الثاني :

الانتشار عبر تلغيم البرامج والصور والفيديو وأي ملف ..

وصل الهاكرز اليوم إلى دمج التروجان في جميع الامتدادات التابعة لبرامج تحتوي أخطاء برمجية ، ولتخطي هذه المشكلة الكبرى يجب أن تثبت أحدث إصدارات البرامج ، وتحدث جميع البرامج الخاصة بك ، سواء برامج الصوت والفيديو أو برامج استعراض الصور ، أو برامج كـ برامج الادوبي مثل فوتوشوب وأكروبات ريدر وافتر أفكت وغيرهم .

لأن الشركة وفي تطويرها لهذه البرامج تقضي على جميع الأخطاء البرمجية والتي قد تمكن الهاكرز من استغلال صيغة يدعمها البرنامج في دمج التروجان بمعنى أكثر وضوحاً لو كانت نسخة الفوتوشوب الخاصة بك قديمة يستطيع الهاكر تلغيم ملف بامتداد PSD وهو امتداد مشهور يتعامل معه برنامج فوتوشوب .

لذلك حاول التحديث المستمر ومن مواقع مشهورة ، هذا بالإضافة لاستمرار عمل كافة الطبقات في تشغيل الملفات المحملة حديثاً من الإنترنت .

وإذا أردت معرفة عملية دمج بسيطة نتابع :

كلنا لدينا برنامج WinRAR ، وهو برنامج خاص بالضغط موجود لدى الأغلب إن لم يكن الجميع .







١ – نختار إنشاء ملف ذاتي التنفيذ .

٢ – نضغط متقدم لإظهار الخيارات الإضافية .





١ – نكتب اسم الملف الأول مع الامتداد .

٢ – نكتب اسم الملف الثاني مع امتداده .

٣ – نضغط أنماط لرؤية الخيارات الخاصة بالتشغيل .



١ ـ نختار إخفاء الكل .

٢ – نذهب لقائمة تحديث .



١ – نختار الكتابة على كافة الملفات .

٢ – إذا أردنا تغيير أيقونة الملف الناتج نذهب للنص والأيقونة .



تم شرح هذا الجزء ، حتى ندرك أن عملية الاختراق سهلة جداً ، وأصبحت هذه التكنولوجيا الخطيرة في أيدي أناس متخلفين ومرضى نفسيين يستخدموها ضد الجميع حتى أقرب المقربين ، وهم في الغالب مخترقين لمن هم أكبر فمثلما يتجسسون على غيرهم يتم التجسس بل وأكثـر .!!!

وحسبنا الله ونعم الوكيـل .

طبعا في عملية الدمج تستطيع دمج أي شيء مع أي شيء يعني تروجان مع فيديو مع صورة أي شيء مع أي شيء .

وطبعا هذه أبسط طرق الدمج وذكرتها لأقول بأن الاختراق سهل جداً ويحتاج خبرة بسيطة سيتم شرحها بالتفصيل في الكتاب القادم ، حتى نسلم من شرور أعدائنا .

سيتم شرح مواضيع كبيرة وطويلة عن علم الاختراق الأخلاقي إن شاء الله في الإصدار الثاني ،

أرجو للجميع الدعاء لي بالانتهاء منه على خير .

وفقنا الله وإياكم لما يحب ويرضى .

الدرس الثالث :

نصائح هامة لجميع مستخدمي الإنترنت ..

- لا تحاول التحميل أبداً من مواقع الشات أو المجموعات أو المدونات المشبوهة والمواقع الغير موثوق فيها .
- استخدم جميع الطبقات بلا استثناء إذا أردت ضماناً جيداً لنفسك .
- استخدم شبكة إنترنت خاصة بك ، أو ثق تماما بكل مستخدمي الشبكة لأن من على الشبكة يستطيع التجسس على كل ما يصدر من جهازك أو يأتي إلى جهازك بكل سهولة ومن الصعب جداً تأمين هذه المعلومات لأنها معلومات داخلية .
- استخدم دائما وأبدا أحدث إصدارات البرامج ، وحاول تحميلها وتثبيتها من مواقعها الرسمية ولا تحاول اختيار البحث في الصفحات العربية ، لأنها في الغالب إما مدموجة أو منقولة عن مواقع أجنبية تم تلغيم البرامج فيها .
- حاول دائما أن تدقق في كل ما يصلك ولا تحاول فتح كل موقع يتم إرساله لك عبر أي وسيلة كانت .
- في حال وصول بعض الرسائل لبريدك الالكتروني إياك أن تحاول فتح رسالة دون التأكد من مصدرها جيداً ، ولا تحاول تحميل وفتح المرفقات في الرسالة لأنها غالباً ملفات فيروسية .
- اعتمد على تطوير الخبرة الخاصة بك دائما ، اكتب اسم البرنامج الغريب عليك في قوقل واكتب بجواره كلمة شرح ، وإذا لم تجد العرب قد شرحوه ، فاعتمد على مترجم قوقل في تصفح المواقع التي قد تشرح وحتماً ستجد شرح في إحدى المواقع العالمية والتي تستطيع بكل سهولة دخولها لو كانت بأي لغة في العالم .
- تذكر أنك بوابة لغيرك ، وغيرك بوابة لك ، حاول التدقيق في كل ما يمر عليك من أحبائك وأصدقائك وافحص وحلل ، ولا تكن سريع الملل .. !!
- تعامل مع المعلومة التي تقتطفها بشكل كريم ، فمثلما أكرمك الله برؤيتها ساهم بأن يراها غيرك ويتعلم منك ، فكما زاد أجري سيزيد أجرك ، والدال على الخير كـ فاعله

- تجنب استخدام أسمائك الشخصية في البريد الالكتروني الخاص بك ، أو في أسمائك على المنتديات وإن حدث وأضافك أحد قد يهددك بأي وسيلة فلا تهتم له ، فهو غالباً سيطبق عليك الكثير من وسائل الهندسة الاجتماعية حتى يستطيع اختراق عقلك ومن ثم اختراق جهازك .
- تذكر أن تثق في قدراتك ، وتعمل على تعلم المزيد دائماً فهذا الكتاب تم كتابته الآن وقد يحدث بعد لحظات اكتشافاً جديداً في عالم متسارع لا يرحم سريع الملل ..!!
- حاول أن تسجل في المنتديات العربية وتطور تفكير الأعضاء بشكل مستمر ، حاول أن تبحث عمن تسأله ويرد بصدر رحب ، لا يهمه المقابل الدنيوي ، حاول تأسيس مجموعة شبابية أخوية من حولك على أرض الواقع لتعلم وتتعلم أكثر ، وحاول نشر العلم للصغار قبل الكبار فالإحصائيات تؤكد على وجود عدد ليس بقليل من الصغار على الانترنت .
- لا تستهن بأبسط الأفكار اطرحها على الجميع وطورها ونفذها ، فقد تكون في البداية تحتاج إلى بعض التنقيح والتعديل ، إلا أنها حتما ستسجل تغييرا في روتين حياتك الذي أتيقن من أنه ممل :)
- علم كل من يجلس على حاسوبك الشخصي على هذه البرامج وطور ثقافة كل من تحب وتحرص عليه ، وتذكر دوما ما دعانا إليه ديننا الحنيف .
- لست إنسانا ملائكيا لا أخطئ ، بل قد أكون أكثر الخطاءين ولكني أطمح لأن أكون أكثر التوابين ، دائما احرص على تصحيح الخطأ حتى لو وقعت ضحية أحدهم وتم سرقة شيء عزيز يخصك حاول أن تلجأ إلى من أعزنا ويعزنا سبحانه جل وعلا ، وإني لمتيقن أن تجد لديه ضالتك .
- كثير من الإخوة والأخوات يتم اختراقهم وسرقة أشياء عزيزة عليهم أو تصويرهم أو غير هذه الأمور ، تأكد إن لم تكن تعرف هذا الهاكر على الطبيعة فمن الصعب جدا التخلص منه ، إن قام بتهديدك فاستخدم معه الهندسة الاجتماعية كما استخدمها معك ، وتذكر قد تكون الحاجة دفعت بعضهم لذلك ، وقد تكون بعض الأمراض النفسية حاول استثارة عواطفه وتذكيره بالآخرة ، فقد يهديه الله ويحذف في لحظة كل ما أخذه منك ومن غيرك ، ولا تحاول استخدام اقصر الطرق في محاولة الاتصال بأي أحد ، وعرض المال وغير ذلك لأن هذا سيقود الهاكر للطمع وسيعرف أن المال الذي يفتقده ويبحث عنه من السهل جداً أن تفرط فيه ، فسيستمر في إيذائك وإيذاء غيرك .

صراحة هناك الكثير من النصائح والتي سأسردها بإذن الله في الجزء القادم بعد شرح الدروس الناقصة هنا ، وإن شاء الله سأحاول وضع كل ما أعرف في شروحات كتابية وصوتية ومرئية على أمل أن أكون ولو من أقل من يقدموا لرفعة هذه الأمة وتغيير عالمها لأفضل الأفضل ..

بارك الله في كل من ينشر الكتاب ، وفي كل من يحاول نشر ولو بعضا من معلوماته ، وبارك الله في كل من يحاول الإضافة عليه ، وجميع حقوق الكتاب للمسلمين عامة ، أجري سيصلني حتى لو قام أحد بتعديل اسم الكاتب ، فأنا أعلم أن من يسجل الأجر رب يعلم ما تكنه الصدور .

اللهم وفقنا ، وعلمنـــا ، وارزقنـــا الشهادة في سبيلك .

الخاتمة

قد يقول قائل ما هذه المعلومات البسيطة ، أما آخر فقد يستصعب من بعض الأمور ، وآخر قد يقول ليس عندي الوقت الكافي للقراءة .

في كل الأحوال فلقد أرضيت ضميري ولله الحمد ، وأتمنى أن يصل كتابي ويستفيد به ولو شخص واحد على مستوى المتحدثين باللغة العربية .

ولا أريد من وراءه أجراً ، فأجري بإذن الله سأستلمه ممن خلق البشر وقسم الأرزاق ، ولكن .

ما أريده حقاً أن يتقن الكثيرين علم وفن الحماية وأساليبها وطرائقها .

وأن يخرج علينا بعض القادة أو المؤسسات أو الجمعيات أو الحكومات أو أي شخص مدعم بمال ووقت وخبرة لإدارة مؤسسة عربية لحماية المستخدمين العرب ، والله الحلم الأكبر أن تقام مؤسسة تدعم الفكر العربي لحماية المستخدمين العرب على شبكة عالمية وضخمة موجودة في كل شيء الآن ومتحكمة في حياتنا ، وتطور البرمجيات التي من شأنها إنقاذ الكثير من وحل الوقوع في ما نرجو الله أن يستره .

أتمنى من كل قلبي أن يتم العمل على مؤسسة عربية عالمية لها مركز وفريق برمجي يعملون المشروع التالي :

بناء موقع ضخم على الإنترنت يحوي منهاج دراسي من الصفر للمستخدم العربي ، مع إضافة برامج عربية الصنع مجانية التوزيع ، يتم نشرها بلا مقابل للجميع لأن الكثيرين ليس معهم ثمن رغيف الخبز فما بالك ببرنامج على الإنترنت .

المهم أن يتم دعم هذا الموقع من أي مؤسسة كانت ، مع فريق تقنى وتطويري يهدف لنشر الموقع بأكثر من لغة عالمية ، وصدقوني أنه سينتشر سريعاً وسيصبح من أقوى المواقع العالمية ، وإني لأتنبأ أن ينافس كبرى المواقع العالمية .

أتمنى كما يتمنى الكثيرون وننتظر تحقيق بعضاً من أحلامنا ، فأصبحنا اليوم نرضى بجزء الجزء ، ونعيش داخل أقفاص تم صنعها بواسطتنا ، ونتعلم من أمسنا أن الغد ما هو إلا تكرار لليوم ، وأننا (جزء) في عالم لا نقوى على تعديل أنفسنا داخله ، فكيف بتعديله هو .

ألا تكفي تضحيات الكثيرين من القادة والمفكرين وحتى الشباب العادي في العالم العربي ، ألا تكفينا صرخات الأطفال في عديد من الدول العربية ، والأفريقية وتهديد

اليهود ، والأمريكان والصليبيين لنا ، ألا يكفينا ما حدث أمام أعيننا من مآسي مازالت تحدث وستحدث لقادة الأمة وشبابها في أكثر من موقع ، فهذا يشنق وذاك يهدد بدور سيدور حتماً على الصامت عنه .

أرجو كما يرجو الكثير من الشباب العربي أن نكون جزءا من تغيير حاضرنا الذليل ، والذي مازلنا فيه مؤثرين على أنفسنا فقط ، نسحبها من الإحباط لليـأس ، ومن الحقيقة إلى أحلام اليقظة ، صدقوني أننا يجب أن نؤمن بقدراتنا ، وبأننا كـ شباب عرب يجب أن ندافع عن إنجازات قام بها الكثيـــر من القادة والعامة في الأمة العربية بهدف تحقيق القوة والمهابة العربية .

أرجو أن لا تنقرض النخوة العربية ، وأن نحييها بأنفسنا ، لا نقول فلندرب الأجيال الصغيرة على قيادة المستقبل ، ففاقد الشيء لا يعطيه .

فلنتدرب على قيادة حاضر الأمة ومستقبلها ، ولا ننتظر ممن يشنق الديمقراطية ويدعم الماسونية مستقبلاً يكتبون في أول حروفه ذلنا ونسيان تاريخنا ، وينسجون قادتنا بأنفسهم ، فلنغير وسنتغير بإذن الله ، لأنه سبحانه وتعالى بشرنا بأن فينا الخير إلى يوم القيامة ، فلنكن على مستوى المسئولية التاريخية ، وكل يعمل من موقعه من أجل غد أفضل لأبنائنا ، لا هم أكبر لهم .. !!

أرجو رجاء حار من جميع من يجد أي خطأ ، أو يريد إضافة أي شيء أن يراسلني على البريد الإلكتروني المذكور ، أو يرسل رسالة نصية لرقم الجوال الخاص بي ، وبإذن الله سيكون الإصدار القادم مرتب ومقسم بشكل أكبر ويحتوي على إضافات وسيتم طرحه بعد تقوم وتنقيح ، بارك الله فيكم جميعاً ، وأجزل لنا ولكم المثوبة .

دمتم بكل خيـر وصحة وسعادة وأمـــن وحماية ..

أخوكم في الله :

حماد موسى حجازي (أبو موسى)

غزة – فلسطين .

تم بحمد الله يوم الجمعة الموافق 18/03/2011



يصعب تجميع المراجع بشكل دقيق ، فالمعلومات تم جمعها من مئات المواقع على الإنترنت والكتب والتجارب الشخصية ، وغيرها الكثير .

لذا سأكتفي في هذه الصفحة بوضع المواقع الرسمية لجميع البرامج ، والمواقع التي تم ذكرها داخل الكتـــاب بالترتيب ::



برنامج الأنظمة الوهمية Microsoft Virtual Machine 2007 SP1

برنامج للبحث عن التعريفات Driver Checker

برنامج للبحث عن التعريفات Driver Genius

الموقع الرسمي العربية Mozilla Firefox

برنامج تجميد النظام الموقع الرسمي Deep Freeze

برنامج مكافح فيروسات الموقع الرسمي Avira AntiVir Personal

جدار ناري الموقع الرسمي FortKnox FireWall

جدار ناري الموقع الرسمي Ashampoo FireWall

برنامج مراقبة النظام الموقع الرسمي Zemana AntiLogger

برنامج تشفير الكتابات الموقع الرسمي KeyScrambler

برنامج تشفير الملفات الموقع الرسمي True Crypt

برنامج رؤية وتحليل برامج بدء تشغيل النظام Autoruns

برنامج يراقب عقل النظام الموقع الرسمي System Shield

برنامج مراقبة تثبيت البرامج الموقع الرسمي Total Uninstaller

برنامج مميز في مراقبة الاتصالات TcpEye

الموقع الرسمي برنامج مميز في مراقبة البرامج والاتصالات Process Hacker

برنامج لالتقاط الهوست الخاص بالهاكرز الموقع الرسمي HeapMemView



موقع مميز وموثوق لتحميل البرامج Download.com

موقع مميز وموثوق لتحميل البرامج Softpedia.com

موقع لإظهار الآي بي الخاص بك ومعلومات عن أي آي بي آخر IpMap.com

مقارنة بين إصدارات الويندوز المختلفة

مقارنة بين أنظمة تشغيل مايكروسوفت من وجهة نظر مايكروسوفت

مقارنة علمية رائعة بين أنظمة تشغيل مايكروسوفت

موقع لإظهار الآي بي الخاص بك Whatipmyip.com

الموقع الرسمي لمتصفح الإنترنت المدعوم من شركة قوقل Google Chrome

معلومات عن الفيروسات من الموسوعة العالمية

موقع الإحصائيات العالمي عن الإنترنت

الموقع العالمي المجاني للتعريفات

إضافة مهمة لمتصفح الإنترنت موزيلا فايرفوكس للتصفح بآيبي آخر TorProxy

مدونتي الخاصة بالدورة

القناة الخاصة بدروس الفيديو الخاصة بالدورة على اليوتيوب

موقع إسلامي رائع وفيه آلاف المواضيع التي تطور الذات وتفسر الواقع